EXHIBIT 32
[FILED UNDER SEAL]

UNITED STATES DISTRICT COURT

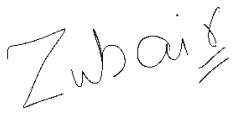
EASTERN DISTRICT OF TEXAS

SHERMAN DIVISION

The State of Texas, et. al. Plaintiff, v. Google LLC, Defendant.	Case No. 4:20-CV-957-SDJ

Rebuttal Expert Report of Professor Zubair Shafiq

September 9, 2024



Zubair Shafiq

Contents

I. INTRODUCTION

A. Assignment

1. My name is Zubair Shafiq, Ph.D. I am an Associate Professor of Computer Science at the University of California, Davis. I have been retained on March 27, 2024, by counsel for the State of Texas, on behalf of all Plaintiff States in this case, to serve as an expert in this litigation to provide rebuttal opinions and testimony regarding whether privacy is a legitimate justification for Google's conduct(s) at issue.

2. This Rebuttal Report contains my opinions in response to the opinions offered by Google's experts and the bases and reasons for my opinions, which I have formulated within a reasonable degree of professional certainty.

3. I have had full access to every document produced in this case and deposition transcripts.[1] I was able to freely conduct searches and review any document and deposition transcript produced in this litigation for the purpose of preparing this Rebuttal Report. I thank my staff at Keystone Strategy, LLC for their assistance in preparing this Rebuttal report. All opinions are my own.

4. I also reviewed public materials, including Google's support pages for Google Ad Manager, Google Ads, and related products at issue in this case.

5. The list of documents and materials I have considered and relied upon are cited inline throughout this Rebuttal Report. The lists are also provided in Appendices A and B.

6. I am being compensated for my work in this case at the rate of $750 per hour. My compensation is not dependent on, and in no way affects, the substance of my opinions. Nor does my compensation depend on the outcome of this proceeding.

7. I understand that document productions are ongoing in this case and that additional relevant documents may be produced in this case by Google and third parties right before and after I issue this report. I may, and reserve the right to, review and rely on additional documents in conducting my work and forming my opinions in this case. I reserve the right to amend or supplement my opinions based on further discovery, information and defendant's experts' testimony provided in this case. I reserve the right to use graphics, figures and/or illustrations at trial to depict conclusions.

[1] I signed a confidentiality order on March 28, 2024, prior to gaining access to Google produced documents.

B. Qualifications

8. I am an Associate Professor of Computer Science at the University of California, Davis, where I lead a research lab focused on online privacy, security, and safety. My lab's research aims to uncover personal data collection, sharing, and usage in the online advertising ecosystem.

9. In addition to my research, I regularly teach undergraduate and graduate courses on computer networks and computer security, including special topics courses covering emerging trends in online advertising and tracking.

10. My research is funded by the National Science Foundation (NSF) through multiple highly competitive research grants. Notably, I am leading the National Science Foundation (NSF) Secure and Trustworthy Cyberspace (SaTC) Frontier Center on Protecting Personal Data Flow on the Internet (ProperData). As part of this effort, my research group is building new device instrumentation systems and measurement methods to investigate personal data collection, sharing, and usage in the web, mobile, and Internet-of-Things (IoT) ecosystems.

11. I have received several awards and distinctions for my research. I am a recipient of the Caspar Bowden Award - Runner-up for Outstanding Research in Privacy Enhancing Technologies (2024), Chancellor's Fellowship (2022-2023), Dean's Scholar Award (2020), National Science Foundation CAREER Award (2018), and Fitch-Beach Outstanding Graduate Research Award (2013).

12. I have co-authored more than 100 peer-reviewed research papers. I received the Best Paper Award at the 2023 ACM Internet Measurement Conference for my research on designing a method to study tracking, profiling, and ad targeting in the Amazon Alexa ecosystem. I also received the 2018 Andreas Pfitzmann Award at the Privacy Enhancing Technologies Symposium for my research on designing a system to detect advertising and tracking data flows in mobile apps. I also received the Best Paper Award at the 2017 ACM Internet Measurement Conference for my research on discovering and studying the abuse of a security vulnerability in Facebook Graph API. I also received the Best Paper Award at the 2012 IEEE International Conference on Network Protocols for my research on reverse-engineering proprietary network protocols.

13. I am the editor-in-chief of the Proceedings on Privacy Enhancing Technologies (PoPETs). I am on the steering committee of the Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb). I am the general chair of the Workshop on Technology and Consumer Protection (ConPro). In the past, I have served as the program chair for the Workshop on Technology and Consumer Protection (ConPro 2022 and 2023) and the Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb 2022 and 2023).

14. My complete CV is attached as Appendix C.

II. SUMMARY OF OPINIONS

15. Based on the evidence that I have reviewed, including publicly available evidence, peer-reviewed research, and internal documents produced by Google in this matter, I conclude that while Google raises unfounded privacy concerns to justify its conduct at issue in this case, Google overlooks far more significant privacy issues to entrench its own data advantage.

16. I offer the following three rebuttal opinions in response to the opinions offered by Defendant's experts Drs. Hoffman, Milgrom, Baye, and Ghose: [2,3,4,5]

    a. First, I disagree with Defendant's experts Drs. Hoffman, Milgrom, and Baye who opine that Google redacted specific fields from the Bid Data Transfer ("BDT") files due to privacy concerns.[6] Defendant's experts offer no basis to justify the privacy concerns from letting a publisher join Data Transfer ("DT") files for the ad auctions happening on the publisher's own website. Defendant's experts ignore the fact that Google reversed the redaction of the fields without any mitigations to address the purported privacy concerns. Similarly, I disagree with Defendant expert Dr. Ghose that Google's restrictions on Header Bidding were justified by privacy concerns.[7] It is my opinion that there are no unique privacy concerns with Header Bidding as compared to Google's Open Bidding. Dr. Ghose fails to identify any unique privacy concerns with Header Bidding as compared to Google's Open Bidding.

    b. Second, I disagree with Dr. Ghose's opinions that Google's competitors have similar access to data as Google and that "Plaintiffs' experts overemphasize the power of

---

[2] Expert Report of Donna L. Hoffman ("Hoffman Report"), July 30, 2024
[3] Expert Report of Paul R. Milgrom ("Milgrom Report"), July 30, 2024
[4] Expert Report of Anindya Ghose ("Ghose Report"), July 30, 2024
[5] Expert Report of Michael R. Baye ("Baye Report"), August 6, 2024
[6] I reviewed the Plaintiffs' opening expert report of Dr. Gans ("Gans Opening Report"), in which he opines that Google concealed its true motivation to limit publishers' ability to gain insights on competing exchanges and used user privacy as a pretext. Gans Opening Report, ¶ 688 ("This section explains that Google's true motivation in redacting data for publishers was to remove the ability of publishers to gain insights about their business on competing exchanges through joining the DT files, and ultimately to preference its ad exchange by removing publishers' abilities to compare their performance across competing exchanges and Header Bidding. Google concealed these motivations, however, by falsely claiming the changes were made in the interest of user privacy.")
[7] Ghose Report, ¶ 22 ("While portraying header bidding as a technological advancement, Plaintiffs' experts gloss over header bidding's significant drawbacks, including latency, domain spoofing, increased risk of ad fraud, privacy issues, billing discrepancies, and self-competition[..]By minimizing these drawbacks, Plaintiffs' experts fail to recognize how Google's Open Bidding addressed some of them, while providing publishers with another way to transact with advertisers.")

Google's data."[8] Contrary to Google's representations to the Federal Trade Commission ("FTC") and Congress "[t]hat data is owned by the customers, publishers and advertisers, and DoubleClick or Google cannot do anything with it,"[9,10] Google joins user browsing data it collects via DoubleClick from publishers' websites to the personal information of Google account holders collected from Google owned and operated ("O&O") websites and products (e.g., Google Search, YouTube, Maps, Chrome). It is my opinion that Google has substantial and unique access to data through its O&O websites and products that provides it with a data advantage over competitors. It is simply not true that competitors have access to "similar" data. Further, Google's advantage is compounded by Google's joining of that data with that of DoubleClick. Recall from above that Google did not allow publishers to join DT files containing auction data on their own websites due to purported privacy concerns. The purported privacy concerns from letting a publisher join auction data on its own website pale in comparison to Google joining data from across millions of non-Google websites and Google O&O websites and products. While a publisher is joining data due to its first-party relationship with a user, Google is leveraging third-party data that it does not own to entrench its own data advantage. Dr. Ghose ignores these privacy concerns and downplays the data advantage that Google gains over its competitors due to its strategic decision to join data it collects from millions of non-Google websites and Google O&O websites and products.

c. Third, I disagree with Dr. Hoffman's opinion that "Google's privacy controls and disclosures empower consumers to customize what they share and the types of ads they see based on their preferences."[11] Dr. Hoffman overlooks the fact that Google's purported privacy controls are riddled with dark patterns that are designed to deceptively

[8] Ghose Report, ¶ 184

[9] Drummond, D., "An examination of the Google-DoubleClick merger and the online advertising industry: what are the risks for competition and privacy? Hearing before the subcommittee on antitrust, competition policy and consumer rights of the Committee on the Judiciary United States Senate One Hundred Tenth Congress First session," (September 27, 2007) https://www.govinfo.gov/content/pkg/CHRG-110shrg39015/html/CHRG-110shrg39015.htm. Accessed August 23, 2024. ("Again, no control over the advertising, no ownership of the data that comes with that that is collected in the process of the advertising. That data is owned by the customers, publishers and advertisers, and DoubleClick or Google cannot do anything with it.")

[10] FTC, "Statement of FEDERAL TRADE COMMISSION Concerning Google/DoubleClick FTC File No. 071-0170" (December 20, 2007), https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf. (p. 12) ("However, the customer and competitor information that DoubleClick collects currently belongs to publishers, not DoubleClick. Restrictions in DoubleClick's contracts with its customers, which those customers insisted on, protect that information from disclosure, and we understand that Google has committed to the sanctity of those contracts.")

[11] Hoffman Report, Section VII ("Given varying preferences for data sharing and ad personalization, Google's privacy controls and disclosures empower consumers to customize what they share and the types of ads they see based on their preferences.")

manipulate user choice. Dr. Hoffman also does not deny that Google's disclosure that "we never sell your personal information to anyone" is misleading. Contrary to Google's disclosure statement, Google sells user data billions of times every day in real-time bidding ("RTB") auctions. Google does not offer any control to users to opt-out of the sale of their data in RTB.

III. GOOGLE'S CONDUCT RELATED TO BID DATA TRANSFER FILES AND HEADER BIDDING CANNOT BE JUSTIFIED BY PRIVACY

17. In their opening reports, Plaintiff's experts Dr. Gans and Dr. Pathak opine on Google's decision to redact certain fields in the BDT files.[12,13,14] Dr. Gans opines that Google's true motivation was to limit publishers' ability to gain insights on competing exchanges and Header Bidding, and that Google used privacy as a pretext.[15] In this section, I analyze and respond to the opinions of Defendant's experts attempting to justify Google's decision to redact certain fields in the BDT files in the name of privacy, including the following:

---

[12] Gans Opening Report, Section VII.D ("Google redacted key publisher data fields in order to suppress the adoption of Header Bidding. Google's claim that it redacted data based on privacy concerns is pretextual. Data redactions harmed competition in the ad exchange market, and reduced publishers' ability to effectively manage their inventory.")

[13] Gans Opening Report, ¶ 677 ("Google redacted valuable information that enabled publishers to evaluate and compare the performance of their inventory across different exchanges. Specifically, Google removed critical information from databases provided to publishers through DFP, rendering it impossible for publishers to know how much bidders on different exchanges were bidding for particular ad inventory, and impossible to evaluate the relative performance of exchanges more generally. Deleting this data for publishers, therefore, harmed competition amongst exchanges, as publishers simply could not evaluate their options of where to sell their inventory without this information. [..] Google only made such redactions because Google had monopoly power in the ad server market and was vertically integrated into the exchange market. Google's monopoly power and vertical integration gave it both the ability and the incentive to redact valuable data that would otherwise be available to publishers and enable greater competition amongst exchanges. Thus, this conduct harmed competition, specifically the ability to compare prices across exchanges, and harmed publishers' operations.")

[14] Plaintiffs' opening expert report of Dr. Pathak ("Pathak Opening Report"), ¶ 150 ("In addition, Google broke DFP publishers' ability to measure the performance of Header Bidding. Google provides two types of data files to DFP publishers: Data Transfer files, which include Header Bidding bids, and a Bid Data Transfer file, which includes AdX and Exchange bidding bids, commonly referred to as 'DT' files. Google broke the link that allowed publishers to compare the results of these files. Externally, Google described this breakage as about protecting user privacy. However, internally, Google described the data redactions as preventing publishers from determining what advertisers were willing to pay for impressions, which diminishes the utility of the data. [redacted] described the purpose of breaking the DT files as to block the 'ability to use the joinability to create user lists, which could be sold downstream directly to DMPs (data management providers) or target those users in Header Bidding or reservations.' The redaction of the DT protected AdX against the threat of Header Bidding because it removed publishers' ability to measure Header Bidding results and effectively target users.")

[15] Gans Opening Report, ¶ 688 ("Google's true motivation in redacting data for publishers was to remove the ability of publishers to gain insights about their business on competing exchanges through joining the DT files, and ultimately to preference its ad exchange by removing publishers' abilities to compare their performance across competing exchanges and Header Bidding. Google concealed these motivations, however, by falsely claiming the changes were made in the interest of user privacy. It further obscured its motivations by also claiming that these were necessary in light of its move to a first-price auction format.")

a. Dr. Hoffman opines that Google made changes to certain fields in BDT files that prevented publishers from tying the data in these files to individual users.[16] Dr. Hoffman goes on to suggest that Google's changes were consistent with consumers' preferences that the data not be used to identify them.[17]

b. Dr. Baye opines that Google redacted certain data fields in BDT files to prevent publishers from tying bid data back to individual users.[18,19] Dr. Baye concludes that these changes were made due to contractual obligations and privacy considerations.[20] Dr. Baye concedes that these changes would diminish the utility of data for publishers, but states that Google added new fields to make up for it.[21,22]

c. Dr. Milgrom opines that Google redacted certain data fields in the BDT files to ensure "that Google fulfilled its contractual commitments, addressed the privacy concerns of its buyers, and also shared a more complete set of bids with its publisher customers."[23,24] Dr.

[16] Hoffman Report, ¶ 66 ("I understand that, in 2019, Google made changes to certain data files that it shares with certain publishers as part of its ad auction process. I also understand that the 2019 changes prevented publishers from combining certain of these files and therefore prevented data in these files from being tied to individual users.")
[17] Hoffman Report, ¶ 66 ("The inability to tie data to specific consumers is consistent with consumer preferences. Specifically, there is evidence from academic literature that consumers generally prefer, when data about them is shared with others, that the data cannot be tied back to them or used to identify them, and consumers are more willing to share data when it is shared in this way.")
[18] Baye Report, ¶ 578 ("In parallel with the shift to the new form of BDT files, Google redacted and adjusted certain data fields in these files to prevent bids from being tied back to individual users.")
[19] Nitish Korula Deposition (April 19, 2024) (p. 38) ("We also changed the structure of the data transfer files, so certain information that could be personally identifying information was removed.")
[20] Baye Report, ¶ 578 ("These changes, which were the result of contractual obligations and privacy considerations, made the new BDT files unjoinable with other auction data files that Google provides publishers.")
[21] Ibid, ¶ 578 ("Recognizing that the redaction and the resulting break in joinability would diminish the utility of data, Google included additional data fields to 'make up for the reduced usefulness.'")
[22] Ibid, ¶ 579 ("By January 2020, Google included additional data fields based on closed beta feedback and allowed all remaining publishers on GAM360 to subscribe to the new BDT files at an additional monthly fee of $1,200.")
[23] Milgrom Report, ¶ 494 ("Google modified BDT files to prevent linking between losing bids and end-user data while also 'remov[ing] the option for bidders to opt out of including information about their bids[.]' These combined changes ensured that Google fulfilled its contractual commitments, addressed the privacy concerns of its buyers, and also shared a more complete set of bids with its publisher customers."); Also supported by Nitish Korula Deposition (04.19.2024) (p. 37) ("We made several changes to the auction[..]including a change from a second-price auction to a first-price auction. As part of those changes, we wanted to provide publishers more visibility into the full set of bids that they got, but we also had to balance that against some other constraints such as privacy and legal constraints.")
[24] Ibid, ¶ 512 ("Instead, he attempts to support his conclusion by quoting a single document that states, "We want to prevent a publisher being able to determine 'these advertisers were willing to pay this much for that user's impression.'" However, rather than providing support for his conclusion, that quote aligns with the historical context I have provided regarding Google's concerns for user privacy, its contractual commitments, and its desires to share the bids of more buyers with publishers.")

Milgrom further underplays the significance of these redactions by suggesting that publishers could use alternatives.[25]

A. Contrary to the assertions of Google's experts, Google had no legitimate privacy concern to redact fields in BDT files.

18. Defendant's experts predominantly rely on the declaration of [redacted] to justify Google's redaction of certain fields in BDT files due to privacy concerns.[26,27]

19. [redacted] states in his declaration that "there were privacy concerns that certain types of bid data could be tied to individual users if BDT files containing a more complete set of bids could be combined with other types of Data Transfer ["DT"] files."[28]

20. [redacted] further states that, in September 2019, Google keyed BDT files in a way that they could not be joined, and removed other fields that could have been used to join different DT files.[29] Specifically, Mr. Berntson describes two main changes: (1) Google "changed the 'KeyPart' field in BDT files to be unique to those files and not joinable with other Data Transfer report files" and (2) Google "removed other fields that otherwise could have been used to probabilistically join BDT files with other Data Transfer report files."[30]

21. In the first change to the "KeyPart" field, [redacted]"[31]

22. In the second change, [redacted]

[25] Ibid, ¶ 513 ("Furthermore, publishers wishing to 'evaluate the performance of exchanges in Header Bidding' had alternatives to acquire relevant information. For example, publishers could use A/B tests or experiments to evaluate how key performance indicators would change in the presence of certain Header Bidding exchanges.")
[26] [redacted]
[27] Milgrom Report, ¶ 494, 511, 514; Hoffman Report, Footnote 129
[28] [redacted]
[29] Ibid
[30] Ibid
[31] [redacted]

data at the hour level meant that publishers could no longer precisely match bids with an impression using timestamps."[32]

23. The privacy concern described by Defendant's experts and [redacted] that the data could be tied to individual users is unsupported. [redacted] and Defendant's experts offer no evidence that a publisher actually tied or could have tied the data in the joined DT files to individual users.

24. It is also worth recognizing that, even if it were possible for a publisher to tie data to individual users by joining different DT files, the publisher would identify the user who is visiting the publisher's website.[33] In other words, even if one assumes that it is theoretically possible, the publisher is only able to tie data to individual users on its own website.

B. Google reverted the redactions in BDT files without addressing the purported privacy concerns.

25. Earlier in 2024, Google reverted the redactions and brought back the key fields into the BDT files. If privacy were the driving concern when Google initially redacted these fields in BDT files in 2019, Google would not have simply reverted the changes in 2024 without implementing other mitigations.

26. [redacted] states that "In January 2024, Google made available to publishers using Google Ad Manager 360 a modified Bids Data Transfer report file - the Joinable Bids Data Transfer report file ("Joinable BDT file") - that could be joined with other Data Transfer report files containing bid information."[34]

27. Google released the new version of BDT files in 2024 stating that it "added a new bids Data Transfer file type that is joinable to all other Data Transfer files. This file includes details about all bids (excluding bids to EEA users) for your inventory, whether the bid won the auction or not."[35] Specifically, Google reverted the two changes from 2019: (1) it updated the "KeyPart" field such that it can again be used to join bids in

---

[32] [redacted]

[33] When a user visits a publisher's website, they enter into a first-party relationship with the publisher, where the user is effectively the publisher's customer. This relationship is analogous to a customer entering a physical storefront, where the customer expects the store owner to recognize them without perceiving it as an invasion of privacy. In contrast, Google operates as a third party in this interaction, with the customer often unaware that Google is monitoring their activity. It is not Google's role to intervene in the publisher's efforts to identify and understand their own customers.

[34] [redacted]

[35] Google, "2024 Google Ad Manager release archive: January 29 New joinable Bids Data Transfer file," https://support.google.com/admanager/answer/14438060#zippy=%2Cjanuary-new-joinable-bids-data-transfer-file. Accessed August 19, 2024.

BDT files to other DT files and (2) it updated "Time" and "TimeUsec2" fields to contain the same fine-grained timestamp information as before.[36,37,38]

28. Google internal documents produced in this matter and depositions of Google employees fail to add any further color to the 2024 reversion of the BDT field redactions. When reverting the changes, Google provided no explanation about how it addressed the purported privacy concerns, which Google had used as a justification for these redactions in 2019.[39]

29. Google's unexplained about-face shows that privacy was not a legitimate justification for the redactions to the BDT files.[40]

C. Google was aware of the reduced usefulness of the redacted BDT files and therefore built a communications plan around user privacy.

30. A Google internal presentation dated July 24, 2019, and marked confidential, reveals Google employees revisiting its first price ("1P") auction transparency narrative [redacted] Employees at Google were aware of the reduced usefulness of redacted BDT files to inform pricing strategy and that the redaction would be disruptive for publishers.[43] Anticipating public relations escalations, Google decided to mitigate the risk by "messag[ing] the change as necessary to protect **user-privacy."** (emphasis in original)[44]

---

[36] Google, "Bids (joinable) data in Data Transfer," https://support.google.com/admanager/answer/13947328. Accessed August 19, 2024. ("The KeyPart field can be used to join bids to other Backfill data transfer files (such as NetworkBackfillRequests and NetworkBackfillImpressions) and can join with the BackfillKeyPart field in non-Backfill files (such as NetworkRequests and NetworkImpressions), since there may be bids on requests that go unfilled or are filled by other line item types.")

[37] Ibid ("Time: The time of the event in your network's local timezone, displayed in 24-hour format (YYYY-MM-DD-HH:MI:SS).")

[38] Ibid ("TimeUsec2: The Unix time (also known as epoch time) of a query in microseconds since 1970-01-01 00:00:00 UTC. Use this value with the Keypart field value to uniquely identify a request or bid auction.")

[39] Google, "2024 Google Ad Manager release archive: January 29 New joinable Bids Data Transfer file," https://support.google.com/admanager/answer/14438060#zippy=%2Cjanuary-new-joinable-bids-data-transfer-file. Accessed August 19, 2024.

[40] Simply put, this situation is akin to a parent restricting their children from playing in the backyard. Imagine a parent who tells their children that they must not play in the backyard because it is dangerous. The children accept this reasoning at face value and adhere to the parent's directive. However, a week later, the parent suddenly asks the children to play in the backyard without any explanation to previously mentioned danger. The children are left wondering whether the parent's concerns about the backyard were valid.

[41] [redacted]

[42] [redacted]

[43] [redacted]

[44] [redacted]

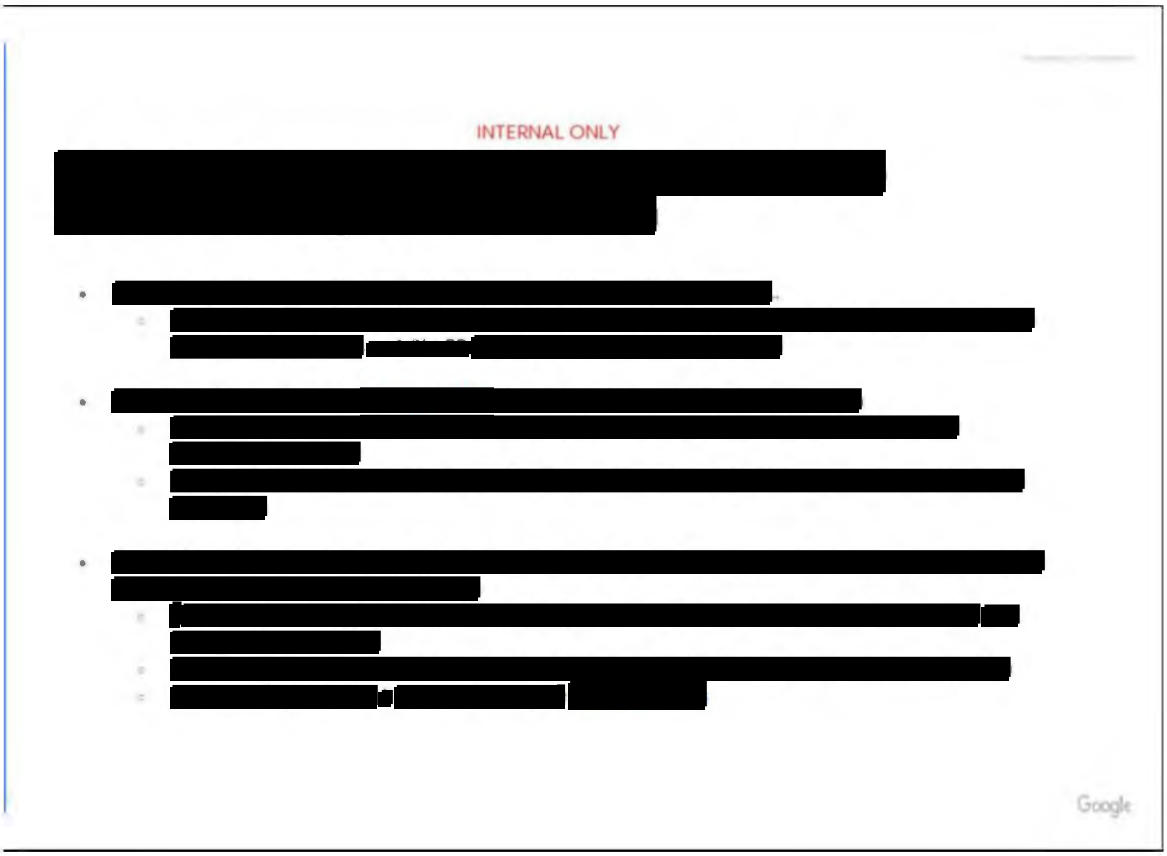


Figure 1: Google employees revisit 1P auction transparency strategy[45]

[45]

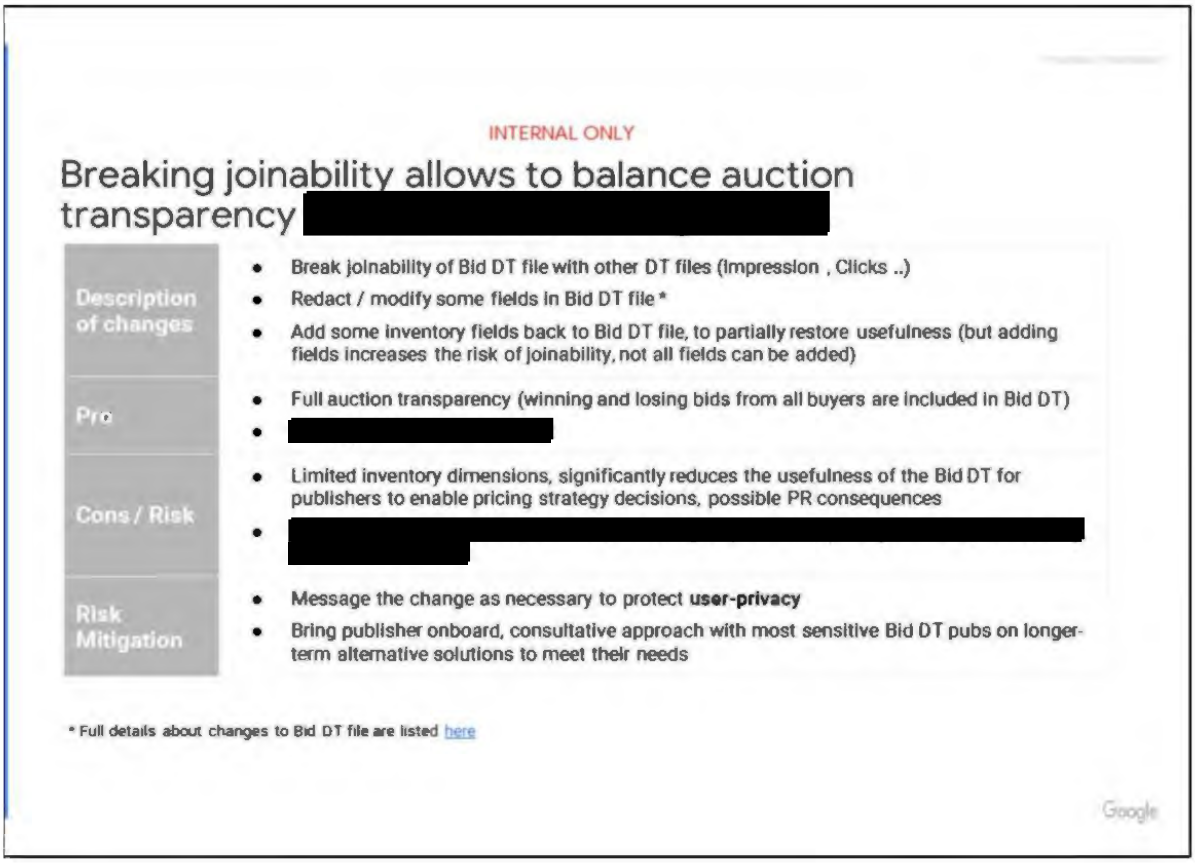


Figure 2: Google's plan to break joinability of BDT files[46]

31. Google also received feedback from publishers that the publishers would be disappointed by Google's redactions to the BDT files and that publishers would not be able to mirror common inventory setups to meaningfully set floors.[47,48,49] At the time of these discussions in 2019, Google employees were aware that, for publishers to effectively manage price floors across demand sources, they needed to see losing AdX and Open Bidding bids when competing exchanges found through Header Bidding won an auction.[50]

[46] [redacted]
[47] [redacted]
[48] [redacted]
[49] Identified evidence contradicts statements in Nitish Korula Deposition (April 19, 2024) ("Q. How did publishers react to changes to that bid data transfer file? A. I think a few publishers expressed some concerns, but I think the vast majority of publishers did not.")
[50] Google internal presentation, "1P Auction – Bid Data Transfer Roll-out plan," (July 24, 2019) GOOG-NE-06879156 at '167 (HCI) ("To manage floor across all indirect demand sources, need to see losing AdX/ EB bids when Header Bidding wins. Today it's done by joining with impression files. Will not be possible in the future")

32. After Google implemented the redactions, Google's internal correspondence shows that it received complaints from publishers who "weren't completely convinced with the user privacy protection narrative."[51]

33. The lack of justification for Google's BDT file redactions along with cited evidence—including Google's internal reference to its messaging as a "narrative"—indicates that Google's true intention for the BDT file redactions was not to protect user privacy.

D. In terms of privacy, Open Bidding is not better than Header Bidding.

34. Defendant's expert Dr. Ghose argues that "While portraying Header Bidding as a technological advancement, Plaintiffs' experts gloss over Header Bidding's significant drawbacks, including [..] privacy issues [..]," which "impact not only advertisers and publishers, but internet users as well. By minimizing these drawbacks, Plaintiffs' experts fail to recognize how Google's Open Bidding addressed some of them, while providing publishers with another way to transact with advertisers."[52] I disagree with Dr. Ghose. Header Bidding does not present any unique privacy concerns as compared to Google's Open Bidding.

35. Dr. Ghose asserts that "Header Bidding increased the risk of data leakage (meaning the unauthorized transmission of user data)."[53] He states that "the user data needed for effective targeting are exposed to all bidders" in Header Bidding.[54] Dr. Ghose fails to recognize that Google's Open Bidding similarly shares user data with bidders in Open Bidding.[55] For example, just like Header Bidding, Google's Open Bidding shares user information such as a user's cookie ID, the latitude and longitude of a user's location, and the URL of the page with bidders.[56,57,58] Both Header Bidding and Google's Open Bidding send bid requests with similar data fields to bidders.

---

[51] Google internal conversation, GOOG-DOJ-29427368 at '368-002 [redacted])

[52] Ghose Report, ¶ 22

[53] Ibid, ¶ 261

[54] Ibid, ¶ 261

[55] Google, "Process the Request," https://developers.google.com/authorized-buyers/rtb/request-guide. Accessed August 19, 2024. ("Bid requests sent to exchange and network bidders participating in Open Bidding are similar to those of Authorized Buyers participating in standard real-time bidding.")

[56] Google, "OpenRTB Integration," https://developers.google.com/authorized-buyers/rtb/openrtb-guide. Accessed August 19, 2024.

[57] Google, "Cookie Matching," https://developers.google.com/authorized-buyers/rtb/cookie-guide. Accessed August 19, 2024.

[58] Plaintiff's opening expert report of Dr. Matthew Weinberg ("Weinberg Report"), ¶ 149 & Figure 29 ("To illustrate the process of Exchange Bidding, suppose there is opportunity to serve an impression for a user over the age of 25 who likes running, and with further fine-grained data from cookies noting that the user has recently visited several shoe-shopping websites, lives in a wealthy neighborhood, and competes in races. Before DFP executes, header bidding solicits bids from exchanges.")

36. Therefore, I conclude that, in terms of privacy, there is no difference between Header Bidding and Google's Open Bidding. Beyond this, Dr. Ghose does not elaborate on the privacy concerns associated with Header Bidding, nor does he provide evidence for how Google's Open Bidding specifically addressed the alleged privacy concerns with Header Bidding.[59]

IV. GOOGLE HAS A SUBSTANTIAL DATA ADVANTAGE OVER ITS COMPETITORS THAT GOOGLE REINFORCES THROUGH PRIVACY-RELATED JUSTIFICATIONS

37. In his opening report, Plaintiff's expert Dr. Gans opines about Google's data advantage as compared to its competitors.[60,61] In this section, I respond to the opinions of Defendant's expert Dr. Ghose, who downplays Google's data advantage over its competitors.

38. Dr. Ghose states that "Plaintiffs' experts contend that Google has access to large volumes of user data that put its competitors with less data at a substantial disadvantage, but they fail to recognize that there are many competitors in display advertising that also have access to large volumes of similar data. Furthermore, and as Plaintiffs' experts recognize, Google's access to data does not preclude others from having similar data, too."[62] Dr. Ghose states that "Plaintiffs' experts overemphasize the power of Google's data."[63] Dr. Ghose further states that there is "no basis for claiming that Google has 'exclusive access' to unique user data."[64]

39. As an initial point, I disagree with Dr. Ghose's opinion that "Plaintiffs' experts overemphasize the power of Google's data." The FTC recognized in 2007 that "[t]he popularity of Google's search engine and its technical prowess already give Google abundant customer information even pre-transaction."[65] More recently, in the FTC's brief submitted on August 12, 2024, for the Epic Games Inc. v. Google LLC et al., case, the FTC discussed how data is a feedback loop that creates a barrier to entry within digital platforms.[66] The FTC states, "When consumers use digital platforms to interact with other users or stakeholders, the platform operator typically retains important data about users and how they behave. As the incumbent

---

[59] Header Bidding is an open-source platform running on the client-side and any potential issues could have been addressed by a server-side implementation of Header Bidding. None of Header Bidding's concerns were insurmountable and needed an alternative such as Open Bidding.
[60] Gans Opening Report, ¶ 363 ("DFP collects a large volume of user and transaction data giving. This data gives DFP a competitive advantage over any potential new entrants. Publisher ad servers need to acquire data to facilitate the ad selection process and enable publishers to manage and control their inventory.")
[61] Ibid, Section V.C.3 ("Google's data advantage is a barrier to entry.")
[62] Ghose report, ¶ 165
[63] Ibid, ¶ 184
[64] Ibid, ¶ 187
[65] Federal Trade Commission, "Statement of Federal Trade Commission concerning Google/DoubleClick FTC File No. 071-0170," (December 20, 2007) https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf. Accessed August 20, 2024. (p. 12)
[66] Sussman et al., "FTC AMICUS CURIAE BRIEF CASE NOS. 3:21-md-02981-JD; 3:20-cv-05671-JD," (August 12, 2024) https://www.ftc.gov/system/files/ftc_gov/pdf/ftc_amicus_brief_epic_v_google_play.pdf. (p. 9-10) Accessed August 28, 2024.

amasses users it therefore also amasses data, which further raises switching costs for users and advertisers. As with network effects, the collection of user data can form a self-reinforcing feedback loop: users engage with a platform, providing data to that platform, and the platform takes advantage of that data to further draw and lock-in users, advertisers, and other stakeholders to the platform. This continuous loop creates a barrier to entry."[67,68] As I discuss in detail later in the section, Google's inherent data advantage and its decision to join first-party and third-party data compounds Google's data advantage.

40. Google has a data advantage which stems from (1) its size and (2) its unique access to data that is available only to Google through its ownership of multiple products and services, such as Google Search, YouTube, Google Maps, Google Chrome, Gmail, Google Shopping, Google Travel, Google Hotels, Google Flights, Google Translate, Google News, etc.

41. It is important to recognize Google's dominance in the United States in collecting data both as a first party (i.e., Google O&O data from Google Search, YouTube, Google Maps, etc.) and as a third-party (i.e., on non-Google websites through, e.g., DoubleClick).

    a. Google collects first-party data on various Google O&O websites, which dominates that of its competitors. For example,

        i. Google Search (www.google.com) is the most popular search engine, with 88% market share.[69]

        ii. YouTube (youtube.com) is the most popular social media and video streaming service, with 81% market share.[70]

---

[67] Martin, N., "How Much Does Google Really Know About You? A Lot," https://www.forbes.com/sites/nicolemartin1/2019/03/11/how-much-does-google-really-know-about-you-a-lot/. Accessed August 29, 2024.
[68] Stigler Committee on Digital Platforms, "Final Report," (September 2019) https://research.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf?la=en&hash=2D23583FF8BCC560B7FEF7A81E1F95C1DDC5225Eh Accessed August 28, 2024. (p. 40). ("Barriers to equivalent data resources, a side effect of not having the history, scale, or scope of the incumbent, can inhibit entry, expansion, and innovation. The same effects that drive the quality of digital services higher as more users join—a positive feedback loop—makes the strong stronger and the weak weaker. Data feeds the development of algorithmic and AI training processes that enables more profitable exploitation of consumer attention through advertising. A data advantage over rivals can enable a company to achieve a virtuous circle of critical economies of scale leading to network effects, and a competitive balance in its favor, leading to the gathering of yet more data. A new entrant is likely to experience this in reverse—a vicious cycle—as it fails to surmount the entrance barrier.")
[69] statcounter, "Search Engine Market Share United States of America," https://gs.statcounter.com/search-engine-market-share/all/united-states-of-america. Accessed September 6, 2024.
[70] Auxier, B., Anderson, M., "Social Media Use in 2021," https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/. Accessed August 19, 2024.

iii. Google Maps (maps.google.com) is the most popular maps service, with 72% market share.[71]

b. Google Chrome (google.com/chrome) is the most popular web browser, with 52% market share in 2024.[72] Google Chrome has a sync feature to collect and join all browsing history and other data (e.g., bookmarks) across devices to a user's Google account.[73] In an internal email conversation in 2020, Google employees estimate there are 175 million Chrome sync users in the U.S. (~53% of US population).[74]

c. Google's third-party data collection covers approximately three-quarters of all websites, which is much more comprehensive than any other company.

i. In 2015, Libert conducted research that found that Google tracks users on 78.07% of the top one million websites. [75]

ii. In 2022, Dambra et al. conducted research that found that Google tracks users on 72.33% of the websites within the researchers' dataset of 2.35 million websites.[76,77] According to this research, Google's third-party data collection coverage is 2.7 and 17.6 times more than that of Meta and Microsoft, respectively.[78] Dambra et al. found that Google tracked 99.76% of the 250,000 users in their dataset once every 1.11 hours on average.[79,80] The authors went on

---

[71] Statista, "Most popular mapping apps in the United States as of April 2018, by reach," https://www.statista.com/statistics/865419/most-popular-us-mapping-apps-ranked-by-reach/. Accessed August 19, 2024.
[72] Statista, "Market share of leading internet browsers in the United States and worldwide as of August 2024," https://www.statista.com/statistics/276738/worldwide-and-us-market-share-of-leading-internet-browsers. Accessed September 5, 2024.
[73] Google, "Sign in and sync in Chrome," https://support.google.com/chrome/answer/185277?hl=en&co=GENIE.Platform%3DDesktop. Accessed September 6, 2024.
[74] Google internal conversation, "Re: Action Items from early meeting," GOOG-AT-MDL-001079596 at '597 ("After talking to Chrome analysts [redacted] we were advised to rely on magic eye estimates of gaia users of chrome sync (which is ~260M gaias) and use deflation factor of 1.5 [redacted] to account for multiple gaias per user which gives us an estimate of 175M chrome users in the US.") (CI)
[75] Libert, T. (2015). "Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 million Websites." In the International Journal of Communication, Volume 9, pp 3544-3561. https://ijoc.org/index.php/ijoc/article/view/3646/1503 ("Corporate Ownership")
[76] Dambra et al. (2022). "When Sally Met Trackers: Web Tracking from the Users' Perspective." In the 31st USENIX Security Symposium 2022 (USENIX Security 22). https://www.usenix.org/conference/usenixsecurity22/presentation/dambra (p. 2191)
[77] Ibid (p. 2193)
[78] Ibid (p. 2193)
[79] Ibid (p. 2191)
[80] Ibid (p. 2193)

to conclude that it is not realistic for a user to fully prevent being tracked by Google.[81] Specifically, the authors stated that "Google, for instance, is encountered on average every 1.11 hours. This means that to fully prevent the largest company in our dataset from being involved in tracking practices, a user should delete the cookies after every single browsing hour, which is obviously not realistic."[82] The authors found that Google is "the only company that also covers many less popular websites that do not receive many visits."[83]

iii. Ghostery's research based on data from five million real users found that Google tracks users on 72% of web traffic.[84,85] According to this research, Google's third-party data collection coverage is 4.2, 5.1, and 6.5 times more than that of Amazon, Meta, and Microsoft, respectively.[86]

iv. DuckDuckGo's research found that Google tracks users on 78.8% of the websites.[87] According to this research, Google's third-party data collection coverage is 3.8, 2.9, and 2.3 times more than that of Amazon, Meta, and Microsoft, respectively.[88,89,90]

v. In 2016, Englehardt and Narayanan's research found that Google tracks users on more than 75% of the top one-million websites.[91] The authors found that "All of the top 5 third parties, as well as 12 of the top 20, are Google-owned domains."[92]

---

[81] Ibid (p. 2196)
[82] Ibid (p. 2196)
[83] Ibid (p. 2192)
[84] Ghostery is a free and open-source company creating privacy and security-related anti-tracking and ad-blocker browser extensions.
[85] Ghostery, "GHOSTERY WHOTRACKS.ME: Uncover who is tracking you online with WhoTracks.Me, featuring statistical reports derived from the web's largest open-source database of trackers," https://whotracks.me/. Accessed August 19, 2024.
[86] Ghostery, "ORGANIZATION TRACKING REACH The chart illustrates the online tracking landscape across various organizations, depicting the extent of their reach," https://www.ghostery.com/whotracksme/tracking-reach. Accessed September 6, 2024.
[87] DuckDuckGo, "tracker-radar/entities/Google LLC.json," https://github.com/duckduckgo/tracker-radar/blob/main/entities/Google%20LLC.json. Accessed August 19, 2024.
[88] DuckDuckGo, "tracker-radar/entities/Amazon Technologies, Inc..json," https://github.com/duckduckgo/tracker-radar/blob/main/entities/Amazon%20Technologies%2C%20Inc..json. Accessed August 29, 2024.
[89] DuckDuckGo, "tracker-radar/entities/Facebook, Inc..json," https://github.com/duckduckgo/tracker-radar/blob/main/entities/Facebook%2C%20Inc..json. Accessed August 29, 2024.
[90] DuckDuckGo, "tracker-radar/entities/Microsoft Corporation.json," https://github.com/duckduckgo/tracker-radar/blob/main/entities/Microsoft%20Corporation.json. Accessed August 29, 2024.
[91] Englehardt, S., Narayanan, A. (2016). "Online tracking: A 1-million-site measurement and analysis." In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). DOI: https://doi.org/10.1145/2976749.2978313
[92] Ibid (Section 5.1)

42. During Google's acquisition of DoubleClick in 2007, the FTC anticipated privacy and competition concerns stemming from Google's own data advantage when coupled with additional data that Google would have access to through DoubleClick.[93,94] Specifically, the FTC recognized the risks of Google's data advantage and its ability to leverage the same, stating:

    a. "Finally, we assessed the suggestion that the combination of Google's database of user information and the data respecting users and competitive intermediaries collected by DoubleClick on behalf of its customers would give Google an overwhelming advantage in the ad intermediation market. The popularity of Google's search engine and its technical prowess already give Google abundant customer information even pre-transaction. However, the customer and competitor information that DoubleClick collects currently belongs to publishers, not DoubleClick. Restrictions in DoubleClick's contracts with its customers, which those customers insisted on, protect that information from disclosure, and we understand that Google has committed to the sanctity of those contracts."[95]

    b. "The transaction will combine not only the two firms' products and services, but also their vast troves of data about consumer behavior on the Internet [...] The online advertising market already is characterized by several different types of network effects. By purchasing DoubleClick, Google will acquire data that will contribute to, and exacerbate, network

[93] Federal Trade Commission, "Statement of Federal Trade Commission concerning Google/DoubleClick FTC File No. 071-0170," (December 20, 2007) https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf. Accessed August 20, 2024. (p. 12) ("Finally, we assessed the suggestion that the combination of Google's database of user information and the data respecting users and competitive intermediaries collected by DoubleClick on behalf of its customers would give Google an overwhelming advantage in the ad intermediation market. The popularity of Google's search engine and its technical prowess already give Google abundant customer information even pre-transaction. However, the customer and competitor information that DoubleClick collects currently belongs to publishers, not DoubleClick. Restrictions in DoubleClick's contracts with its customers, which those customers insisted on, protect that information from disclosure, and we understand that Google has committed to the sanctity of those contracts.")

[94] Jones Harbour, P., "In the matter of Google/DoubleClick F.T.C. File No. 071-0170 DISSENTING STATEMENT OF COMMISSIONER PAMELA JONES HARBOUR," (December 20, 2007) https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf. Accessed August 20, 2024. (p. 4, 5& 7) ("The transaction will combine not only the two firms' products and services, but also their vast troves of data about consumer behavior on the Internet [..] The online advertising market already is characterized by several different types of network effects. By purchasing DoubleClick, Google will acquire data that will contribute to, and exacerbate, network effects. As a result, the Google/DoubleClick combination is likely to 'tip' both the search and display markets in Google's favor, and make it more difficult for any other company to challenge the combined firm [..] The combined Google/DoubleClick will be able to exploit network effects and accelerate a convergence between search and display. Various scenarios for data sharing have been hypothesized, but they all rely on the same conclusion: search information gathered by Google, combined with browsing information gathered by DoubleClick, will create a far richer source of data to enable highly targeted advertising.")

[95] FTC, "Statement of FEDERAL TRADE COMMISSION Concerning Google/DoubleClick FTC File No. 071-0170," (December 20, 2007) https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf. (p. 12).

> effects. As a result, the Google/DoubleClick combination is likely to 'tip' both the search and display markets in Google's favor, and make it more difficult for any other company to challenge the combined firm. [...] The combined Google/DoubleClick will be able to exploit network effects and accelerate a convergence between search and display. Various scenarios for data sharing have been hypothesized,[96] but they all rely on the same conclusion: search information gathered by Google, combined with browsing information gathered by DoubleClick, will create a far richer source of data to enable highly targeted advertising."[97]

43. In response to the FTC's concerns, Google made representations to the FTC and Congress, stating "[t]hat data [data collected by DoubleClick] is owned by the customers, publishers and advertisers, and DoubleClick or Google cannot do anything with it."[98,99] Google assured regulators that it would not leverage its access to DoubleClick data, stating "[w]e will not combine DoubleClick cookie information with personally identifiable information unless we have your **opt-in consent**." (emphasis in original)[100]

---

[96] Several concerned third parties described the following scenario. Today, DoubleClick places a cookie on a user's computer, which enables DoubleClick to track the user's visits to any website that displays ads served by DoubleClick. Similarly, Google places a cookie on a user's computer to track searches and clicks resulting from searches. Both of these cookies are linked to a computer's Internet Protocol, or IP, address. Some computers with "always on" Internet access keep the same IP address for long periods of time. Other computers change IP addresses periodically. Post-merger, a user would visit one or more sites displaying DoubleClick ads, and also conduct one or more Google searches, during a time period when the IP address remained the same (a highly likely confluence of events, given each party's reach on the Internet). The merged firm would be able to use the common IP address to link the Google and DoubleClick cookies on that machine, and thereby cross-index that user among both databases – without relying on any proprietary customer data. And once the cookies themselves were linked in the merged firm's dataset, it would not matter if the user's IP address changed in the future.

[97] Jones Harbour, P., "In the matter of Google/DoubleClick F.T.C. File No. 071-0170 DISSENTING STATEMENT OF COMMISSIONER PAMELA JONES HARBOUR" (December 20, 2007), https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf. (p. 4, 5& 7)

[98] FTC, "Statement of FEDERAL TRADE COMMISSION Concerning Google/DoubleClick FTC File No. 071-0170," (December 20, 2007) https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf. (p. 12) ("However, the customer and competitor information that DoubleClick collects currently belongs to publishers, not DoubleClick. Restrictions in DoubleClick's contracts with its customers, which those customers insisted on, protect that information from disclosure, and we understand that Google has committed to the sanctity of those contracts.")

[99] Drummond, D., "An examination of the Google-DoubleClick merger and the online advertising industry: what are the risks for competition and privacy? Hearing before the subcommittee on antitrust, competition policy and consumer rights of the Committee on the Judiciary United States Senate One Hundred Tenth Congress First session," (September 27, 2007) https://www.govinfo.gov/content/pkg/CHRG-110shrg39015/html/CHRG-110shrg39015.htm. Accessed August 23, 2024. ("Again, no control over the advertising, no ownership of the data that comes with that that is collected in the process of the advertising. That data is owned by the customers, publishers and advertisers, and DoubleClick or Google cannot do anything with it")

[100] Google internal presentation, "Narnia2 Townhall 2016-08-23," (August 23, 2016) GOOG-NE-11433745 at '747 (HCI)

44. Subsequently, as described next, Google reversed course and joined DoubleClick and Google data. Google's decision to join DoubleClick and Google data contradicts the representations Google made to the FTC and Congress. Google did leverage its access to data from DoubleClick by joining user data it collected from different publisher websites via DoubleClick with user data from Google's O&O websites.[101] This decision compounded Google's data advantage over its competitors.

45. In 2016, with a project internally referred to as Narnia2, Google made an explicit choice to combine Google's O&O data with the data it collected from non-Google websites via DoubleClick.[102]

46. A presentation titled "Narnia2 Townhall" explains that Google changed its privacy policy from "We will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent" to "Depending on your account settings, your personal information may be combined with your browsing data - the content you see on the web and in apps - in order to improve Google's products and the ads you see both on and of Google."[103]

47. To implement this change, Google prompted existing users to opt-in by means of deceptive practices—also called "dark patterns"—while Google opted new users in by default.[104,105] The information given to users was vague, with titles like "[s]ome new features for your Google account."[106] Google did not clearly notify users that they were consenting to Google joining DoubleClick browsing data it collects from millions of non-Google websites to the personal data of Google account holders.

48. An internal Google document from 2016 confirms that the privacy policy statement underwent the aforementioned change.[107] The goal of the change was to "create a single view of the users' signed-in identity and data throughout [Google's] product and advertising systems."[108] To get "consent," Google's plan was to invasively "bump" existing users with a screen to accept Google's new privacy policy.[109,110]

---

[101] Google Internal Presentation, "Narnia2 Townhall 2016-08-10," (August 10, 2016) GOOG-NE-10944631 at '709 (CI) ("Summary: Narnia2 Unified view of the user across O&O and 3rd party site activity")
[102] Ibid
[103] Ibid at '640 (CI)
[104] A dark pattern is a User experience (UX) design pattern that might manipulate the user into agreeing to something that might not be in their best interest (for example giving away personal information) or, more generally, discourage informed, intentional decision making. "Dark patterns" are also referred to as "deceptive patterns."
[105] Angwin, J., "Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking," https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking. Accessed August 8, 2024.
[106] Ibid
[107] Google internal document, "Narnia 2 Gaia Keyed Serving End State Design (Tinman)," (June 12, 2016) GOOG-AT-MDL-016354429 at '430 (CI)
[108] Ibid at '429 (CI)
[109] Ibid at '429 (CI)
[110] Ibid at '431 (CI)

Meanwhile, newly created accounts were considered "consented" by default.[111] Meaning, new users were opted-in by default.[112] These tactics resulted in a rise in the number of opted-in users who "accepted" Google's new policy of joining DoubleClick browsing data it collects from millions of non-Google websites to the personal data of Google account holders.[113]

49. Google's own documents show that the company knew the 2016 shift to joining DoubleClick and Google O&O data raised major issues regarding consent.[114,115,116] For example, [redacted] described Google's workaround to join DoubleClick and Google O&O data during her deposition:

    a. "So biscotti is the DoubleClick cookie, which is how DoubleClick would represent -- would recognize users across the Internet, and I think there was a consent decree that said that they would not join that cookie with any information that Google got from the owned properties roughly. So if like Google recognized a user and knew what type of things they served for, you could not use that with a DoubleClick cookie [..] Gaia was a replacement for this where basically users would opt in and we would build a different way of recognizing users that would not be using the biscotti cookie anymore and, therefore, it would not be subject to the consent decree. instead of saying like: 'Can we use this data for advertising?' They would say: 'Here's a new feature. If you want it, we can use your information for anything.' [..] not being upfront with users [..] some of the terms had changed[..] gaia refers this other way of getting cookies, and just generally a different way of getting people to identify themselves in a way that Google would have more freedom to use their information. [..] So we can use -- all of our services can use any of the data and we're going to break down some of the silos."[117]

---

[111] Ibid at '431 (CI)
[112] Google Internal Presentation, "Narnia2 Townhall 2016-08-10," (August 10, 2016) GOOG-NE-10944631 at '640 (CI)
[113] In my opinion, Google assumes users' consent to be an indicator that they "accepted" the new privacy policy. However, Google employed deceptive practices to get the consent (namely the invasive "bumps" and default opt-in for new users.)
[114] [redacted]
[115] Google Internal document, "The Obligation to Play Fair Or, Why I'm Leaving Display Ads," (April 10, 2015) GOOG-TEX-00453431 at '431 (HCI) [redacted] "Here are a few examples of where I believe we tilt the playing field to benefit ourselves: [..] most recently, pivoting our focus to gaia instead of biscotti. Biscotti is also known as the DoubleClick Cookie, and our use of it is subject to a consent decree.")
[116] Federal Trade Commission, "In the matter of Google Inc., Corporation – Decision and order," (October 13, 2011) https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf. Accessed August 20, 2024.
[117] [redacted]

50. As an internal presentation from 2016 notes, Google had been very clear in past privacy statements that "[w]e will not combine DoubleClick cookie information with personally identifiable information unless we have your **opt-in consent**." (emphasis in original)[118] However, the presentation later stated that the consent was designed to include "interruptive prompting," which is a known type of a dark pattern.[119,120] Google specifically designed the flow of the "consent bump" for the [redacted] Google account holders to "start as passive voluntary flow" which "soon becomes interruptive prompting users at sign in."[121]

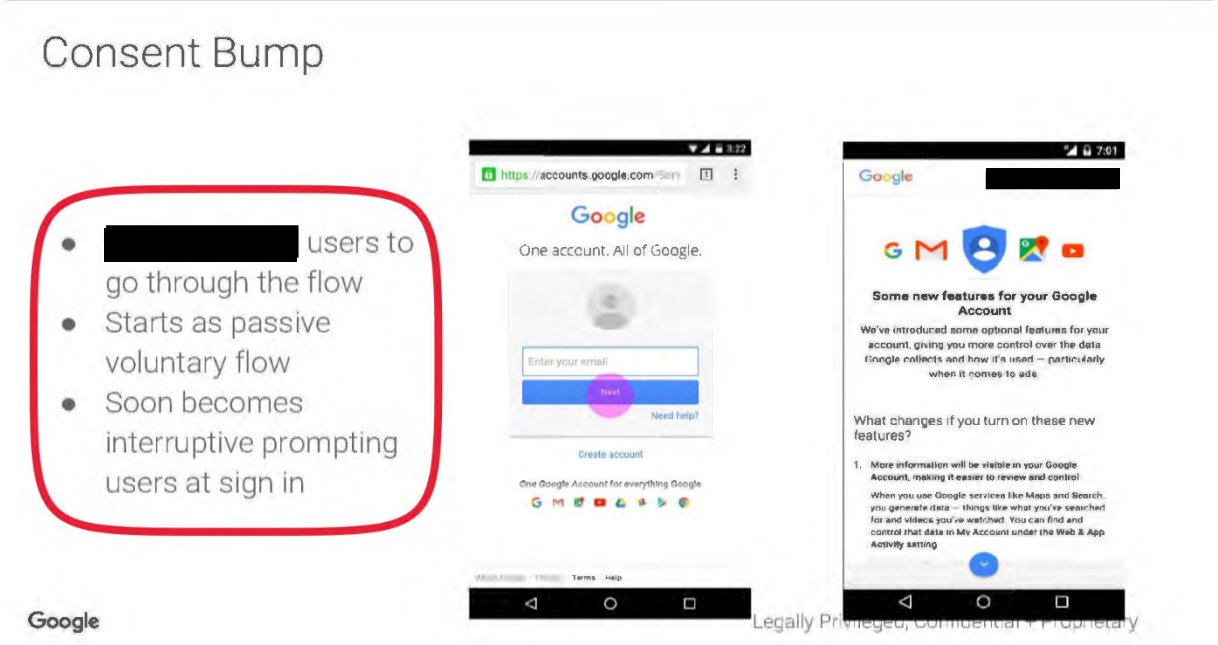


Figure 3: Internal Google presentation showing evolution of "consent bump"[122]

51. In a strategy document, Google employees explain that their goal when launching Narnia2 was to maximize opted-in users [redacted] and minimize opt-out rate [redacted]

[118] Google internal presentation, "Narnia2 Townhall 2016-08-23," (August 23, 2016) GOOG-NE-11433745 at '747 (HCI)
[119] Ibid at '753 (HCI)
[120] Deceptive Patterns, "Nagging," https://www.deceptive.design/types/nagging. Accessed August 19, 2024. ("Nagging (also known as 'interruptive prompting') is a form of adversarial resource depletion. Every time an app or a website interrupts the user with a request to do something, this depletes the user's time and attention. This is like a tax that the provider imposes on users who do not want to comply with the provider's wishes. Although the cost is non-financial, it adds up and eventually becomes non-trivial. At this point, the user may decide that it's more cost effective to just give in and agree to whatever the provider is asking for, even if it is against their best interests.")
[121] Google internal presentation, "Narnia2 Overview 2016-12-14," (December 14, 2016) GOOG-AT-MDL-007418936 at '944 (HCI)
[122] Ibid

[redacted]).[123,124] In periodic updates after launching Narnia2, Google reported that [redacted] and [redacted] which shows that the Narnia2 "consent bump" was specifically designed to achieve a high opt-in rate.[125,126,127]

52. Figure 4 shows a slide from the presentation titled "Narnia2 Townhall 2016-08-23." It illustrates that, from a technical perspective, before this change Google did not combine data it collected from DoubleClick with the data it collected from Google O&O services such as Google Search, YouTube, Google Maps, etc. (the IDs for data from Google O&O services [GAIA ID] and DoubleClick [Biscotti ID] were not linked). But after this change, Google linked the user's browsing data it collected via DoubleClick to the personal information Google collects about consumers on Google O&O services.

[123] [redacted])

[124] [redacted])

[125] [redacted]

[127] Google internal presentation, "Narnia2 Townhall 2016-08-23," (August 23, 2016) GOOG-NE-11433745 at '753 (HCI)

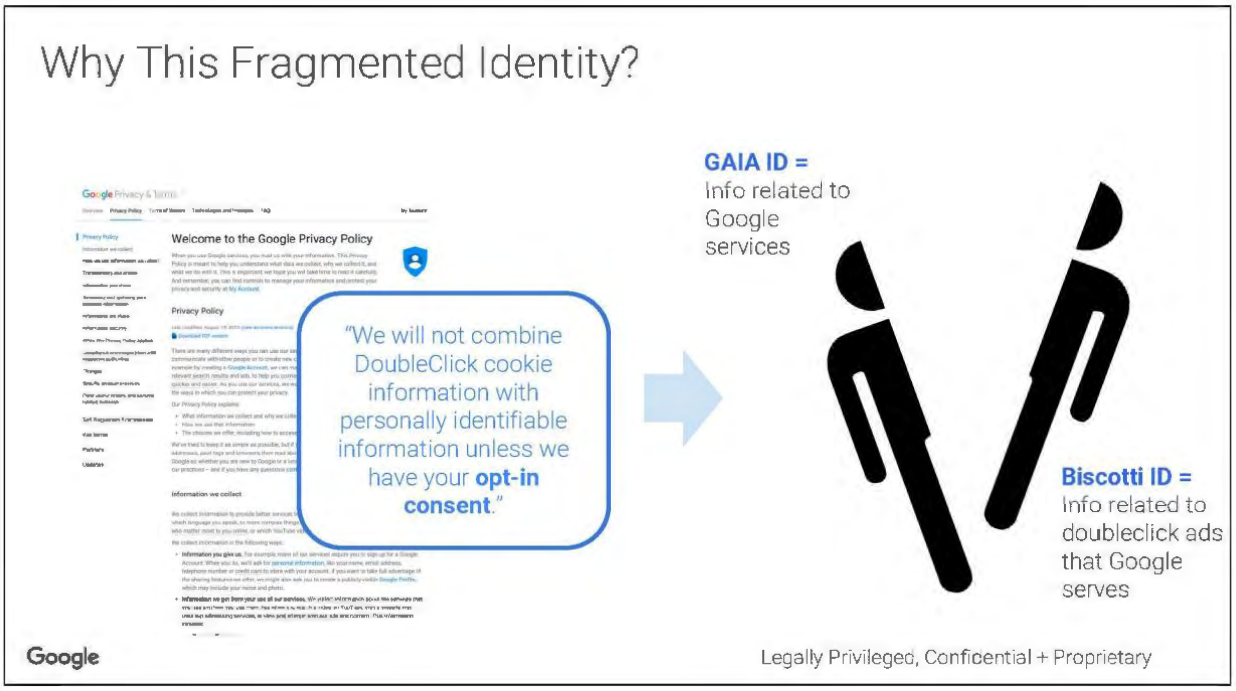


Figure 4: User's fragmented identity before combining data from DoubleClick and Google[128]

53. A 2016 ProPublica article explained that "[t]he practical result of the change is that the DoubleClick ads that follow people around on the web may now be customized to them based on your name and other information Google knows about you. It also means that Google could now, if it wished to, build a complete portrait of a user by name, based on everything they write in email, every website they visit and the searches they conduct."[129] This article's description of Google's capability after it decided to join DoubleClick and Google data is accurate based on my review of the evidence produced in this matter. Later in 2017, Google announced that it will stop scanning email content for ad personalization going forward.[130,131]

[128] Ibid at '747 (HCI)
[129] Angwin, J., "Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking," https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking. Accessed August 8, 2024.
[130] Fung, B., "Gmail will no longer snoop on your emails for advertising purposes," https://www.washingtonpost.com/news/the-switch/wp/2017/06/26/gmail-will-no-longer-snoop-on-your-emails-for-advertising-purposes/. Accessed September 6, 2024. ("Google is making a change to its advertising practices that will affect millions of Gmail users around the globe. Starting later this year, the company will stop reading your emails to refine its ads.")
[131] Greene, D., "As G Suite gains traction in the enterprise, G Suite's Gmail and consumer Gmail to more closely align," (June 23, 2017) https://blog.google/products/gmail/g-suite-gains-traction-in-the-enterprise-g-suites-gmail-and-consumer-gmail-to-more-closely-align/. Accessed September 6, 2024 ("Consumer Gmail content will not be used or scanned for any ads personalization after this change.")

54. Google's strategy documents explain how after joining non-Google and Google data through Narnia2, Google would be able to build more "holistic" user profiles.

    a. [redacted] Narnia2 enables us to tap data across Google properties and marry interest data such as general location history or web history with intent data such as search queries, site/store visits to build a holistic in-depth user profile that understands exactly where the user is in their purchase journey, what they are currently looking for and even predict what type of products they could be interested in the future."[132]

    b. An internal Google conversation describes that a [redacted]"[133]

55. After the launch of Narnia2, Google could now build more holistic or unified profiles to target users with better personalized ads. For example, Figure 5 shows how Google could better target consumers "[i]n-market for Minivans" by combining their Google (e.g., search history in Google Search, location history from Google Maps) and non-Google data (conversion events in Auto Trader app).[134]

[132] [redacted]

[133] Google internal conversation, "Launched: Narnia 2.0/ Signed-in Moment of Consent for Display Ads," (July 18, 2016) GOOG-AT-MDL-012335682 at '683 and '684 (CI)

[134] Google internal presentation, "Narnia2 Overview 2016-12-14," (December 14, 2016) GOOG-AT-MDL-007418936 at '978 (HCI)

Figure 5: Enhanced targeting post Narnia2[135]

56. In addition to Google's reversal on assurances made to the FTC, Google implemented alterations (i.e., redactions) to BDT files based on purported privacy concerns, discussed above in Section III.A, so that publishers could no longer join auction data collected on their own websites. Google's dismissal of privacy concerns when it joined non-Google (DoubleClick) and Google data while restricting publishers' ability to join auction data on their own websites reflects a double standard.[136]

57. By joining DoubleClick and Google data, which was—separately—already more comprehensive than its competitors' data, Google now undoubtedly had the most comprehensive and exclusive data about consumers compared to any of its competitors.[137]

58. Google's decision to join DoubleClick and Google data contradicts the representations Google made to the FTC and Congress. Google's ability to compound and reinforce its data advantage has long been recognized, yet Google reneged on assurances not to leverage its unique access to data while applying a double standard and relying on privacy concerns to limit others.

[135] Google internal presentation, "Narnia2 Overview 2016-12-14," (December 14, 2016) GOOG-AT-MDL-007418936 at '978 (HCI)
[136] Referring back to the analogy I used in Footnote 33, users have a first party relationship with the publisher and do not see it as an invasion of privacy when the publisher is able to identify them.
[137] Google does not share data it collects from Google O&O websites and products with its competitors.

59. Therefore, Dr. Ghose's attempt to downplay Google's data advantage is misleading. The evidence shows that no competitor can rival Google's access to data, and hence, Google's advantaged position to leverage this data.

V. GOOGLE'S PRIVACY DISCLOSURES ARE MISLEADING AND ITS CONTROLS ARE RIDDLED WITH DARK PATTERNS

60. Defendant's expert Dr. Hoffman responds to Plaintiff's allegations that "Google engaged in deceptive trade practices towards advertisers, publishers, and consumers," "Google has used deceptive language when describing its advertising and privacy practices to users," and "Google misleads consumers when it states that 'It Does Not Sell Users' Personal Information."[138] In response, Dr. Hoffman opines that Google offers disclosures and privacy controls to consumers. Dr. Hoffman states that "[g]iven varying preferences for data sharing and ad personalization, Google's privacy controls and disclosures empower consumers to customize what they share and the types of ads they see based on their preferences."[139]

A. Google's privacy controls are riddled with dark patterns.

61. Dr. Hoffman states that "Google provides all consumers—including consumers who do not have a Google account—with tools that allow them to control the information they share with Google and with third parties, to customize the kinds of ads they see, and to change their settings as desired."[140] Dr. Hoffman fails to acknowledge that Google employs deceptive interfaces or dark patterns, which hinder consumers' ability to discover or meaningfully use those controls.[141,142,143] These include, but are not limited to, privacy-unfriendly default settings, hiding privacy-friendly choices, employing misleading wording, and providing choice architectures where choosing privacy-friendly option requires more effort.[144,145,146]

---

[138] Hoffman report, ¶ 19
[139] Ibid, ¶ 24
[140] Ibid, ¶ 47
[141] Referring to my previous description of "Dark patterns" in Section IV Footnote 104, a dark pattern is a user experience design pattern that might manipulate the user into agreeing to something that might not be in their best interest (for example giving away personal information) or, more generally, discourage informed, intentional decision making.
[142] Deceptive Patterns, "What are deceptive patterns?" https://www.deceptive.design/. Accessed August 19, 2024.
[143] Deceptive Patterns, "Hall of shame: Hundreds of examples of deceptive patterns used by companies around the world," https://www.deceptive.design/hall-of-shame?brand=Google. Accessed August 19, 2024.
[144] Google internal document, "Narnia 2 Gaia Keyed Serving End State Design ([redacted] (June 12, 2016) GOOG-AT-MDL-016354429 at '431 (CI)
[145] Tahaei, M., Vaniea, K. (2021). "'Developers Are Responsible': What Ad Networks Tell Developers About Privacy." In Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems (CHI EA '21), Article No.: 253, pp 1–11. DOI: https://doi.org/10.1145/3411763.3451805
[146] Narayanan et al. (2020). "Dark Patterns: Past, Present, and Future: The evolution of tricky user interfaces," ACM Queue, Volume 18, Issue 2. https://dl.acm.org/doi/pdf/10.1145/3400899.3400901 (p. 67-92)

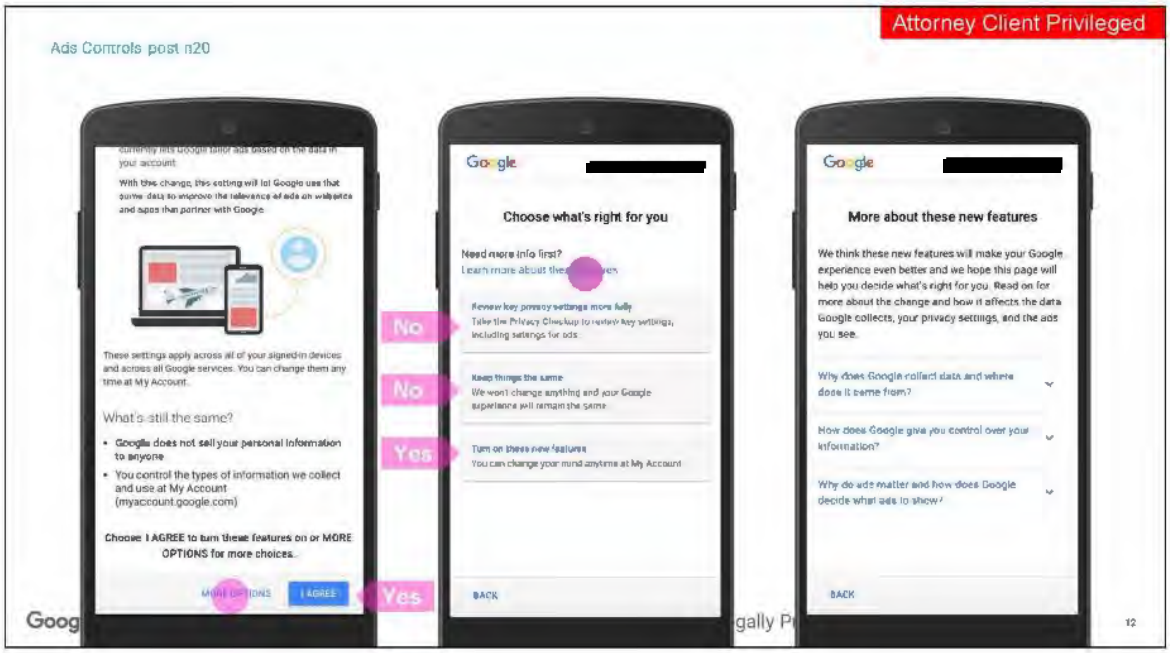


Figure 6: Choosing privacy-friendly option requires users to navigate multiple pages[147]

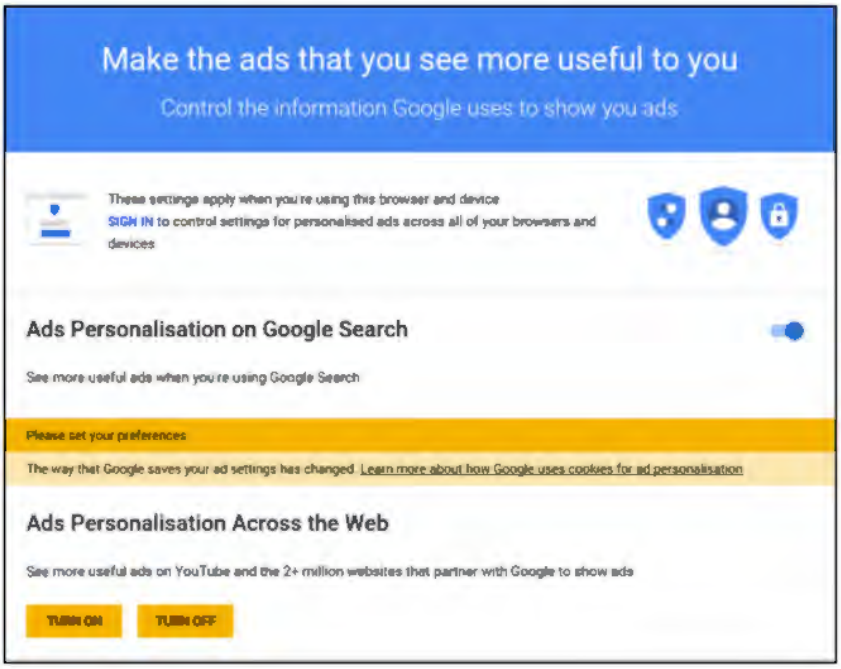


Figure 7: Unclear default settings in desktop version of Google's ads settings[148]

62. In 2021, Tahaei and Vaniea documented various dark patterns used by Google AdMob.[149] The researchers found that Google AdMob's sample code "continues to ask for user consent even if users decline it, which is a clear example of nagging behavior."[150] Additionally, Google AdMob's sample code provided to website developers "notif[ies] the user about using location without giving them any options to refuse, or providing

consent popups that do not have a 'I do not consent' button."[151] The research found that Google AdMob "uses false hierarchy by making the first option on the consent popup builder not include a 'Do not consent' option, while the second nearly-identical choice does."[152] Lastly, the researchers describe how Google AdMob uses "aesthetic manipulation in the content categories UI by having a blue toggle represent blocked items and a grey one for allowed items."[153]

63. In 2022, the FTC published a staff report that showed how companies, including Google, are increasingly using sophisticated dark patterns that are designed to trick consumers.[154,155] The FTC staff report describes how Google's default settings maximize data collection. For example, "the way [Google] portrayed the choices was in such a manner that you would turn on location tracking."[156] The FTC concluded that "[t]hese dark patterns are often presented as giving consumers choices about privacy settings or sharing data but are designed to intentionally steer consumers toward the option that gives away the most personal information."[157]

64. The Norwegian Consumer Council also documented dark patterns that Google uses to undermine consumer privacy.[158] In 2018, it concluded that "Google's privacy dashboard promises to let the user easily

---

[147] Google Internal Presentation, "Narnia2 Townhall 2016-08-10," (August 10, 2016) GOOG-NE-10944631 at '642 (CI).
[148] The Norwegian Consumer Council, "Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy," (June 27, 2018) https://storage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf. Accessed August 19, 2024. (p.16) ("In the desktop version of Google's ads settings, it is impossible to tell if "Ads Personalisation Across the Web" is turned on or off by default.")
[149] Tahaei, M., Vaniea, K. (2021). "'Developers Are Responsible': What Ad Networks Tell Developers About Privacy." In Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems (CHI EA '21), Article No.: 253, pp 1–11. DOI: https://doi.org/10.1145/3411763.3451805
[150] Ibid (Section 4.5)
[151] Ibid (Section 4.5)
[152] Ibid (Section 4.5)
[153] Ibid (Section 4.5)
[154] Federal Trade Commission, "Bringing Dark Patterns to Light," (September 2022) https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf. Accessed September 6, 2024.
[155] Federal Trade Commission, "FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers: Tactics Include Disguised Ads, Difficult-to-Cancel Subscriptions, Buried Terms, and Tricks to Obtain Data," (September 15, 2022) https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers. Accessed September 6, 2024.
[156] Federal Trade Commission, "Bringing Dark Patterns to Light," (September 2022) https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf. Accessed August 29, 2024.
[157] Federal Trade Commission, "FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers: Tactics Include Disguised Ads, Difficult-to-Cancel Subscriptions, Buried Terms, and Tricks to Obtain Data," (September 15, 2022) https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers. Accessed August 29, 2024.
[158] The Norwegian Consumer Council, "Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy," (June 27, 2018) https://storage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf. Accessed August 19, 2024.

delete user data, but the dashboard turns out to be difficult to navigate, more resembling a maze than a tool for user control."[159]

65. Users who do not wish to allow Google to access data find that opting out of Google's data collection methods is often difficult and confusing. In 2019, the French National Commission on Informatics and Liberty (Commission Nationale de l'Informatique et des Libertés or "CNIL"), the French agency responsible for data protection, fined Google ~$57M for failing to obtain meaningful consent from users to access their data.[160] It found that Google's disclosures are "not easily accessible for users."[161] For instance, "[t]he relevant information is accessible after several steps only, implying sometimes up to 5 or 6 actions. For instance, this is the case when a user wants to have a complete information on his or her data collected for the personalization purposes or for the geo-tracking service."[162] It also found that Google's disclosures are "not always clear nor comprehensive."[163] For instance, it noted that some of Google's disclosures are "too generic and vague."[164]

66. In another case in 2022, CNIL concluded that Google made it difficult for users to reject cookies, fining the company ~$175M.[165] CNIL found that Google allowed users to accept cookies with a single click, whereas those who wanted to refuse cookies had to navigate through several steps.[166,167,168]

67. In another investigation in 2023, the German antitrust authority found that Google's practices had given users insufficient choice in controlling what happened to their data. To end the investigation, Google agreed to change its opt-out practices. As the antitrust authority noted in a summary of the commitments

---

[159] Ibid (p. 3)
[160] Goldsmith, J., "France Slaps Google With €50M Fine For Privacy Violation Under GDPR," https://www.forbes.com/sites/jillgoldsmith/2019/01/21/france-slaps-google-with-e50m-fine-for-privacy-violation-under-gdpr/. Accessed August 16, 2024.
[161] European Data Protection Board, "The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC," https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en. Accessed August 16, 2024.
[162] Ibid
[163] Ibid
[164] Ibid
[165] Vincent J., "France fines Google and Facebook for pushing tracking cookies on users with dark patterns / One button to accept all — but not to reject all," https://www.theverge.com/2022/1/7/22871719/france-fines-google-facebook-cookies-tracking-dark-patterns-eprivacy. Accessed August 8, 2024.
[166] Ibid
[167] Deceptive Patterns, "Deliberation of the Restricted Committee concerning Google LLC and Google Ireland Limited," https://www.deceptive.design/cases/deliberation-of-the-restricted-committee-concerning-google-llc-and-google-ireland-limited. Accessed August 8, 2024.
[168]Commission Nationale de l'Informatique et des Libertés (CNIL – French Data Protection Authority), "Deliberation of the restricted committee No. SAN-2021-023 of 31 of December 2021 concerning GOOGLE LLC and GOOGLE IRELAND LIMITED," (December 31, 2021) https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-023_of_31_december_2021_concerning_google_llc_and_google_ireland_limited.pdf. Accessed August 16, 2024.

Google was undertaking, "Google has to design the choice options in a way that users can provide consent in a freely given, specific, informed and unambiguous manner."[169,170]

68. Google provides a setting where users can opt-out of linking their data across Google sites and apps.[171] This setting is historically hard to find and understand, and most users do not know about it. In 2017, Google data indicated that 90% of all users and 94% of Android users had opted in to linking the data.[172] A year later, Google noted that only 10% of signed-in users opted out of this sharing.[173] More recently in 2022, an internal Google presentation noted that "WAA (an opt-out control) is on for 95% of accounts worldwide."[174]

69. In 2022, commentary on an internal Google presentation explained some of the factors influencing these low opt-out rates. The commentary noted that, "In general users do not interact with opt-out controls."[175] The commentary also noted that one particular setting had only a 1% opt-out rate, and that the company expected another setting on the same page to have an even lower opt-out rate because the "location controls further sit at the bottom of the privacy tab."[176]

70. Google's decision to roll out transparency and control features is in part dependent on the impact on its advertising revenues. For example, in 2021, Google tested features that would give users more control over privacy settings with the goal of "improv[ing users'] privacy sentiment."[177] An internal email conversation shows that the features achieved this, but also increased opt-out.[178] Google employees expressed concern that Google would lose access to these users' data: "I am really hoping we have a long term trend of gaining users who turn on location, turn on personalization as opposed to a narrative where we are losing

---

[169] The Bundeskartellamt, "Decision pursuant to Section 19a(2) sentence 4 in conjunction with Section 32b(1) GWB - Public version," (June 10, 2023) https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2023/B7-70-21.pdf. Accessed August 16, 2024. (p. 20)

[170] Heine, F., "Google changes user data practices to end German antitrust probe," https://www.reuters.com/technology/german-cartel-office-google-users-have-better-control-over-their-data-2023-10-05/. Accessed August 16, 2024.

[171] Google Help, "Find & control your Web & App Activity," https://support.google.com/websearch/answer/54068. Accessed September 7, 2024.

[172] Google internal document, "Status: Draft in Progress," (July 5, 2017) GOOG-DOJ-29373435 at '438 (CI)

[173] [redacted]

[174] [redacted]

[175] Ibid

[176] Ibid

[177] Google internal conversation, "Re: Follow-up re: Privacy Controls on SERP," (April 29, 2021) GOOG-AT-MDL-006114190 at '196 (CI)

[178] Ibid at '194 (CI) ("[W]e do expect any launch that adds entry points to user setting to result in an increase in setting changes [Web App Activity opt-out rate]. This is a balance we will need to be mindful of for transparency and control launches in the future")

users[..]"[179] Google eventually decided to hold off on rolling out the features that increased transparency until further evaluation of the long-term impact on Google Ads.[180]

71. Google was aware of users' challenges in understanding the data Google collected about them. In 2017-2018, Google employees gathered relevant articles and discussed the impact of users' privacy concerns on the brand's health. They conceded the difficulties users faced: "We have a lot of settings today, but it's hard to find them or know what's most important." They also noted that "[t]oday, users do not have great control over how long we keep their search data." The discussion repeatedly considered ways in which Google could "make it **easy to find** the key personalization or privacy settings" (emphasis in original), but also pointed out the tradeoffs involved for the company, at one point simply noting that a benefit to such a proposed action is that users have "more control over their data," and the corresponding risk is that "[w]e have less data."[181]

72. Google was aware that the company's privacy settings were confusing and that users did not understand them. In a 2020 internal presentation on the user experience with consent, settings, and privacy across Google O&O products, commentary noted that users "don't understand what settings are, don't understand the impact of toggling settings on/off, can't find them when they need them, aren't clear on how product- or device-level settings relate to UDC, etc."[182]

73. Google knew that the problems that users had comprehending and controlling data collection persisted. During an internal Google presentation in 2022, Google employees noted that "Users don't understand how or why we use their data, and the fact that [Google is] in the ads business is at the core of the growing distrust. [Google's] current transparency, disclosures and controls are seen as band-aid solutions that do not address user needs."[183]

74. In summary, Dr. Hoffman overlooks the fact that Google's purported privacy controls are riddled with dark patterns designed to deceptively manipulate user choices.

---

[179] Ibid at '190 (CI)

[180] [redacted]

[181] [redacted]

[183] [redacted]

B. Google's privacy disclosure stating that it does not sell user data is misleading.

75. Dr. Hoffman does not deny the allegation, which she sets out to address in her report, that Google misleads consumers when it tells consumers that "we never sell your personal information to anyone."[184,185]

76. Google sells user data to bidders in real-time bidding ("RTB"). The following diagram provides an overview of Google's RTB system where Google sells users' browsing information alongside identifying information such as cookies and IP address.[186]

Figure 8: Google sells user data in RTB[187]

77. In each bid request of a real-time bidding auction, Google shares hundreds of data fields with bidders.[188] The data fields that Google shares in real-time bidding auctions include identifiers (e.g., cookies, device

[184] Hoffman report, ¶ 19 ("In addition to these allegations, the Plaintiff States allege that Google engaged in deceptive trade practices towards advertisers, publishers, and consumers. In particular, the Plaintiff States allege that Google has used deceptive language when describing its advertising and privacy practices to users.16 Specifically, the Complaint alleges that Google misleads consumers when it states that 'It Does Not Sell Users' Personal Information,' stating that Google 'takes user's personal information, displays it to advertisers, who in turn pay Google money for access to that user.'")
[185] Google, "Ads that respect your privacy," https://safety.google/privacy/ads-and-data/. Accessed August 19, 2024. ("We never sell your personal information to anyone, including for ads purposes.")
[186] Google, "Real-time Bidding," https://developers.google.com/authorized-buyers/rtb/start. Accessed August 19, 2024.
[187] Google, "Real-time Bidding," https://developers.google.com/authorized-buyers/rtb/start. Accessed August 19, 2024.
[188] Google, "Authorized Buyers Real-time Bidding Proto," https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide#bidrequest-object. Accessed August 19, 2024.

identifiers, IP address), location (e.g., geographic coordinates derived from IP address), web browsing (full-string URL of the webpage), and device (e.g., detailed configuration such as OS version, device type, device brand, device model).[189] The bidders use this information in RTB bid requests to decide how much to bid. Google RTB conducts billions of auctions selling user data every day.[190]

78. [redacted] well-known data brokers that openly engage in buying and selling user data.[191,192] For example:

a. Lotame sells "instant access to audience segments consisting of billions of cookies and mobile device IDs. We have captured granular data against these cookies and device IDs and packaged it into thousands of highly curated audience segments," including potentially sensitive political audiences based on "party, interest, affiliation, cause, and more." Lotame also claims that "Partners place proprietary Behavioral Collection Pixels (BCPs), allowing us to collect demographic, interest, action, search, purchase intent, and other data points. Our BCPs enable the collection of more than 2 billion data points/day while organizing them into 2.2 thousand categories of human behaviors."[193]

b. Oracle BlueKai sells "BlueKai Curated audiences," which "are aggregated from top data providers in seven key vertical markets such as auto, CPG, travel, financial, and more." The data types sold by BlueKai include "Behavioral, Demographic, Interest, Lifestyle, In-Market, Mobile, Purchase-Based."[194]

---

[189] Ibid
[190] Google internal presentation, "Turn QBR Review of Q2 2013," (August 16, 2023) GOOG-AT-MDL-015644231 at '235 (CI)
[191] Google, "European regulations overview and guidance Ad technology providers," https://support.google.com/admanager/answer/9012903. Accessed August 19, 2024. ("As part of Google's commitment to complying with the General Data Protection Regulation (GDPR), we provide publishers with controls to select which ad technology providers are allowed to serve and measure ads in the European Economic Area (EEA) and the UK, to support ad delivery, ad measurement, and other functions. All providers listed have shared certain information that is required by the GDPR, a link explaining their data usage that you can share with your users as part of your consent flow, and they have agreed to comply with our data usage policy")
[192] Oracle Data Cloud, "2019 Data Directory," https://web.archive.org/web/20210420081301/https://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf. Accessed August 19, 2024.
[193] Ibid (p. 89- 91)
[194] Ibid (p. 7)

79. Google's selling of user data in RTB with foreign entities was of particular concern to a bipartisan group of U.S. Senators.[195,196] The Senators noted that "[f]ew Americans realize that some auction participants are siphoning off and storing 'bidstream' data to compile exhaustive dossiers about them. In turn, these dossiers are being openly sold to anyone with a credit card, including to hedge funds, political campaigns, and even to governments" and that "[t]his information would be a goldmine for foreign intelligence services that could exploit it to inform and supercharge hacking, blackmail, and influence campaigns."[197,198] The Senators sent out letters to ad networks asking "to name the foreign-headquartered or foreign-majority owned firms that they have provided bidstream data from users in the U.S. to in the past three years," and responses revealed several foreign companies.[199,200] Senator Ron Wyden went on to introduce the "Protecting Americans' Data From Foreign Surveillance Act of 2021" in draft form in April 2021,[201] and the "Protecting Americans' Data From Foreign Surveillance Act of 2023" in June 2023, which was "[r]ead twice and referred to the Committee on Banking, Housing and Urban Affairs."[202] This bill "directs the Department of Commerce (in coordination with specified federal agencies) to identify categories of personal data that could be exploited by foreign governments or foreign adversaries and harm U.S. national security if exported, reexported, or in-country transferred in a quantity that exceeds the threshold established by Commerce," and further to "impose appropriate controls on the export, reexport, or in-country transfer of covered personal data, including through interim controls (e.g., informing a person that a license is required)."[203]

---

[195] Cox, J., "Congress Says Foreign Intel Services Could Abuse Ad Networks for Spying," https://www.vice.com/en/article/88aw73/congress-foreign-intelligence-agencies-bidstream-real-time-bidding. Accessed August 19, 2024.
[196] Adalytics, "Is Google sharing data from Americans and Europeans with sanctioned Russian adtech companies?" https://adalytics.io/blog/sanctioned-ad-tech-user-data. Accessed August 19, 2024.
[197] Ron Wyden United States Senator for Oregon, "Wyden, Bipartisan Senators, Question Online Ad Exchanges on Sharing of Americans' Data with Foreign Companies," (April 02, 2021) https://www.wyden.senate.gov/news/press-releases/wyden-bipartisan-senators-question-online-ad-exchanges-on-sharing-of-americans-data-with-foreign-companies. Accessed August 28, 2024.
[198] Cassidy et al., Letter to Sundar Pichai, Chief Executive Officer of Google LLC, (April 1, 2021) https://www.wyden.senate.gov/imo/media/doc/040121%20Wyden%20led%20Bidstream%20Letter%20to%20Google.pdf. Accessed August 28, 2024.
[199] Ibid (p. 1)
[200] Cox, J., "The Hundreds of Little-Known Firms Getting Data on Americans," https://www.vice.com/en/article/hundreds-companies-bidstream-data-location-browsing/. Accessed August 27, 2024.
[201] Ron Wyden United States Senator for Oregon, "Wyden Releases Draft Legislation to Protect Americans' Personal Data From Hostile Foreign Governments," https://www.wyden.senate.gov/news/press-releases/wyden-releases-draft-legislation-to-protect-americans-personal-data-from-hostile-foreign-governments. Accessed August 27, 2024.
[202] Congress.gov, "S.1974 - Protecting Americans' Data from Foreign Surveillance Act of 2023," https://www.congress.gov/bill/118th-congress/senate-bill/1974. Accessed August 27, 2024.
[203] Ibid

80. In summary, contradicting Google's disclosure that Dr. Hoffman sets out to address in her report saying, "[Google] never sell your personal information to anyone,"[204,205] Google in fact does sell user data in RTB. Google does not offer any control to users to specifically opt-out of the sale of their data through RTB.

C. Consumers are unaware of the extent of Google's data collection and selling.

81. Dr. Hoffman states that "Consumers understand the ads they see are based on their personal data, and many consumers are willing to share personal data in exchange for personalized ads."[206] This is contradicted by research that shows that consumers do not actually fully understand the nature and scale of online data collection and selling that companies like Google engage in.

82. According to Pew Research, about 80% of Americans are concerned over the "data use" and "lack of control" by companies such as Google.[207] In a 2012 research paper by Ur et al., the researchers found that consumers perceived behaviorally personalized ads as "creepy" and "privacy invasive," and that a majority "were either fully or partially opposed" to personalized ads.[208] In a 2019 research paper by Weinshel et al., the researchers found that consumers were surprised by the extent of tracking by companies and to see how companies can infer their interests from browsing history.[209] In a 2024 research paper by Reitinger et al., the researchers found that more than 80% of the research participants were uncomfortable with the level of tracking done by companies such as Google.[210]

---

[204] Google, "Ads that respect your privacy," https://safety.google/privacy/ads-and-data/. Accessed August 19, 2024. ("We never sell your personal information to anyone, including for ads purposes.")
[205] Hoffman report, ¶ 19
[206] Hoffman report, Section VI.B (¶ 43-44)
[207] Auxier et al., "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/. Accessed August 8, 2024.
[208] Ur et al. (2012). "Smart, useful, scary, creepy: perceptions of online behavioral advertising," In Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12), Article 4, pp 1–15. DOI: https://doi.org/10.1145/2335356.2335362 (p. 1&7)
[209] Weinshel et al. (2019). "Oh, the Places You've Been! User Reactions to Longitudinal Transparency About Third-Party Web Tracking and Inferencing." In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). https://doi.org/10.1145/3319535.3363200 (pp. 149-166). ("One-third of participants who saw our fully featured interface were surprised by how trackers used their browsing history to infer their interests, and that interests were even inferred in the first place. [..] Even before using our tool, participants were often aware of the existence of online tracking. However, when confronted with detailed descriptions of tracking in their own browsing, they were often surprised by tracking's extent and prevalence. Further, participants who saw detailed information about potential inferences reported greater intentions to take privacy-protective actions.")
[210] Reitinger et al. (2024). "What Does It Mean to Be Creepy? Responses to Visualizations of Personal Browsing Activity, Online Tracking, and Targeted Ads." In Proceedings on Privacy Enhancing Technologies (PoPETs), Volume 2024, Issue 3, pp 715-743. DOI: https://doi.org/10.56553/popets-2024-0101. (p. 727)

83. Google's own research shows [redacted][211] A Google internal survey showed [redacted].[212] Surveyed people [redacted].[213] For example, imagine a person who has recently been diagnosed with cancer and has been researching treatment options and support groups online. Due to their search history, they encounter an ad saying "Are you struggling with cancer? Take our miracle cure!" which is not only invasive but also exploits the person's vulnerability.

84. Dr. Hoffman's own public commentary on this topic shows that she recognizes that consumers are not aware and do not consent to this scale of data collection. In an interview at the "George Talks Business" event series, Dr. Hoffman explains about the extent of user data collected, saying "what is that data about? That's about you. So that's everything that we are all doing in society; our digital footprints, our click streams, our physical footprints, our credit card information, the information marketers have about us, everything you do on social media, and so on" and subsequently opines that "consumers aren't really aware and haven't really given their consent for this level of data to be scraped and captured about them."[214]

85. In summary, consumers are generally unaware of the depth and scale of Google's data collection, selling and usage for ad personalization. Therefore, Dr. Hoffman's conclusion that "Consumers understand the ads they see are based on their personal data, and many consumers are willing to share personal data in exchange for personalized ads" is wrong.[215]

---

[211] [redacted]

[212] [redacted]

[213] [redacted]

[214] Perry, V., Hoffman, D., "George Talks Business- Donna Hoffman," https://www.youtube.com/watch?v=VVYPfmlUwmg (20:31 – 20:54, 21:25 – 21:36). Accessed August 8, 2024.

[215] Hoffman report, Section VI.B (¶ 43-44)

VI. APPENDIX A: MATERIALS RELIED UPON

A. Books and Papers

Dambra et al. (2022). "When Sally Met Trackers: Web Tracking From the Users' Perspective." In the 31st USENIX Security Symposium (USENIX Security 22). https://www.usenix.org/conference/usenixsecurity22/presentation/dambra

Englehardt, S., Narayanan, A. (2016). "Online Tracking: A 1-million-site Measurement and Analysis." In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). DOI: https://doi.org/10.1145/2976749.2978313

Libert, T. (2015). "Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites." In the International Journal of Communication, Volume 9, pp 3544-3561. https://ijoc.org/index.php/ijoc/article/view/3646/1503

Narayanan et al. (2020). "Dark Patterns: Past, Present, and Future: The evolution of tricky user interfaces." In March-April 2020 ACM Queue, Volume 18, Issue 2, pp 67-92. https://dl.acm.org/doi/pdf/10.1145/3400899.3400901

Reitinger et al. (2024). "What Does It Mean to Be Creepy? Responses to Visualizations of Personal Browsing Activity, Online Tracking, and Targeted Ads." In Proceedings on Privacy Enhancing Technologies (PoPETs), Volume 2024, Issue 3, pp 715-743. DOI: https://doi.org/10.56553/popets-2024-0101

Tahaei, M., Vaniea, K. (2021). "'Developers Are Responsible': What Ad Networks Tell Developers About Privacy." In Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems (CHI EA '21), Article No.: 253, pp 1–11. DOI: https://doi.org/10.1145/3411763.3451805

Ur et al. (2012). "Smart, useful, scary, creepy: perceptions of online behavioral advertising." In Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12), Article 4, pp 1–15. DOI: https://doi.org/10.1145/2335356.2335362

Weinshel et al. (2019). "Oh, the Places You've Been! User Reactions to Longitudinal Transparency About Third-Party Web Tracking and Inferencing." In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), pp 149-166. DOI: https://doi.org/10.1145/3319535.3363200

B. Declarations, Depositions and ROG Responses

Declaration of [redacted] and exhibits, GOOG-AT-MDL-C-000073682 (HCI)

Deposition of Nitish Korula (April 19, 2024) and exhibits

Deposition of [redacted] (May 23, 2024) and exhibits

C. Expert Reports

Expert Report of Jacob Hochstetler, PhD (June 7, 2024)

Expert Report of Joshua Gans, PhD (June 7, 2024)

Expert Report of Matthew Weinberg, PhD (June 7, 2024)

Expert Report of Parag Pathak, PhD (June 7, 2024)

Expert Report of Anindya Ghose, PhD (July 30, 2024)

Expert Report of Donna L. Hoffman, PhD (July 30, 2024)

Expert Report of Paul R. Milgrom, PhD (July 30, 2024)

Expert Report of Michael R. Baye, PhD (August 6, 2024)

D. Documents from Production

GOOG-AT-MDL-001079596 (CI)

GOOG-AT-MDL-006114057 (CI)

GOOG-AT-MDL-006114190 (CI)

GOOG-AT-MDL-006545758 (CI)

GOOG-AT-MDL-006554061 (CI)

[redacted]

[redacted]

GOOG-AT-MDL-012335682 (CI)

GOOG-AT-MDL-015436738 (CI)

GOOG-AT-MDL-015644231 (CI)

GOOG-AT-MDL-016354429 (CI)

GOOG-AT-MDL-019120021

GOOG-AT-MDL-B-000883782 (CI)

[redacted]

[redacted]

GOOG-DOJ-29373435 (CI)

[redacted]

[redacted]

[redacted]

[redacted]

GOOG-NE-10944631 (CI)

[redacted]

[redacted]

[redacted]

E. Public Sources

Adalytics, "Is Google sharing data from Americans and Europeans with sanctioned Russian adtech companies?" https://adalytics.io/blog/sanctioned-ad-tech-user-data. Accessed August 19, 2024.

Angwin, J., "Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking," https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking. Accessed on August 8, 2024.

Auxier et al., "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/. Accessed on August 8, 2024.

Auxier, B., Anderson, M., "Social Media Use in 2021," https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/. Accessed August 19, 2024.

Cassidy et al., Letter to Sundar Pichai, Chief Executive Officer of Google LLC, (April 1, 2021) https://www.wyden.senate.gov/imo/media/doc/040121%20Wyden%20led%20Bidstream%20Letter%20to%20Google.pdf. Accessed August 28, 2024.

Commission Nationale de l'Informatique et des Libertés (CNIL – French Data Protection Authority), "Deliberation of the restricted committee No. SAN-2021-023 of 31 of December 2021 concerning GOOGLE LLC and GOOGLE IRELAND LIMITED," (December 31, 2021) https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-023_of_31_december_2021_concerning_google_llc_and_google_ireland_limited.pdf. Accessed August 16, 2024.

Congress.gov, "S.1974 - Protecting Americans' Data From Foreign Surveillance Act of 2023," https://www.congress.gov/bill/118th-congress/senate-bill/1974. Accessed August 27, 2024.

Cox, J., "Congress Says Foreign Intel Services Could Abuse Ad Networks for Spying," https://www.vice.com/en/article/88aw73/congress-foreign-intelligence-agencies-bidstream-real-time-bidding. Accessed August 19, 2024.

Cox, J., "The Hundreds of Little-Known Firms Getting Data on Americans," https://www.vice.com/en/article/hundreds-companies-bidstream-data-location-browsing/. Accessed August 27, 2024.

Deceptive Patterns, "Deliberation of the Restricted Committee concerning Google LLC and Google Ireland Limited," https://www.deceptive.design/cases/deliberation-of-the-restricted-committee-concerning-google-llc-and-google-ireland-limited. Accessed on August 8, 2024.

Deceptive Patterns, "Hall of shame: Hundreds of examples of deceptive patterns used by companies around the world," https://www.deceptive.design/hall-of-shame?brand=Google. Accessed August 19, 2024.

Deceptive Patterns, "Nagging," https://www.deceptive.design/types/nagging. Accessed August 19, 2024.

Deceptive Patterns, "What are deceptive patterns?" https://www.deceptive.design/. Accessed August 19, 2024.

Drummond, D., "An examination of the Google-DoubleClick merger and the online advertising industry: what are the risks for competition and privacy? Hearing before the subcommittee on antitrust, competition policy and consumer rights of the Committee on the Judiciary United States Senate One Hundred Tenth Congress First session," (September 27, 2007) https://www.govinfo.gov/content/pkg/CHRG-110shrg39015/html/CHRG-110shrg39015.htm. Accessed on August 23, 2024.

DuckDuckGo, "tracker-radar/entities/Facebook, Inc..json," https://github.com/duckduckgo/tracker-radar/blob/main/entities/Facebook%2C%20Inc..json. Accessed August 29, 2024.

DuckDuckGo, "tracker-radar/entities/Microsoft Corporation.json," https://github.com/duckduckgo/tracker-radar/blob/main/entities/Microsoft%20Corporation.json. Accessed August 29, 2024.

DuckDuckGo, "tracker-radar/entities/Amazon Technologies, Inc..json," https://github.com/duckduckgo/tracker-radar/blob/main/entities/Amazon%20Technologies%2C%20Inc..json. Accessed August 29, 2024.

DuckDuckGo, "tracker-radar/entities/Google LLC.json," https://github.com/duckduckgo/tracker-radar/blob/main/entities/Google%20LLC.json. Accessed August 19, 2024.

European Data Protection Board, "The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC," https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en. Accessed August 16, 2024.

Federal Trade Commission, "Bringing Dark Patterns to Light," (September 2022) https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf. Accessed September 6, 2024.

Federal Trade Commission, "FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers: Tactics Include Disguised Ads, Difficult-to-Cancel Subscriptions, Buried Terms, and Tricks to Obtain Data," (September 15, 2022) https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers. Accessed September 6, 2024.

Federal Trade Commission, "In the matter of Google Inc., Corporation – Decision and order," (October 13, 2011) https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf. Accessed August 20, 2024.

Federal Trade Commission, "Statement of Federal Trade Commission concerning Google/DoubleClick FTC File No. 071-0170," (December 20, 2007) https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf. Accessed August 20, 2024.

Fung, B., "Gmail will no longer snoop on your emails for advertising purposes," https://www.washingtonpost.com/news/the-switch/wp/2017/06/26/gmail-will-no-longer-snoop-on-your-emails-for-advertising-purposes/. Accessed September 6, 2024.

Ghostery, "GHOSTERY WHOTRACKS.ME: Uncover who is tracking you online with WhoTracks.Me, featuring statistical reports derived from the web's largest open-source database of trackers," https://whotracks.me/. Accessed August 19, 2024.

Ghostery, "ORGANIZATION TRACKING REACH The chart illustrates the online tracking landscape across various organizations, depicting the extent of their reach," https://www.ghostery.com/whotracksme/tracking-reach. Accessed September 6, 2024.

Goldsmith, J., "France Slaps Google With €50M Fine For Privacy Violation Under GDPR," https://www.forbes.com/sites/jillgoldsmith/2019/01/21/france-slaps-google-with-e50m-fine-for-privacy-violation-under-gdpr/. Accessed August 16, 2024.

Google Chrome Help, "Manage your linked Google services," https://support.google.com/chrome/answer/14202892?hl=en&co=GENIE.Platform%3DAndroid. Accessed August 29, 2024.

Google, "2024 Google Ad Manager release archive: January 29 New joinable Bids Data Transfer file," https://support.google.com/admanager/answer/14438060#zippy=%2Cjanuary-new-joinable-bids-data-transfer-file. Accessed August 19, 2024.

Google, "Ads that respect your privacy," https://safety.google/privacy/ads-and-data/. Accessed August 19, 2024.

Google, "Authorized Buyers Real-time Bidding Proto," https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide#bidrequest-object. Accessed August 19, 2024.

Google, "Bids (joinable) data in Data Transfer," https://support.google.com/admanager/answer/13947328. Accessed August 19, 2024.

Google, "Cookie Matching," https://developers.google.com/authorized-buyers/rtb/cookie-guide. Accessed August 19, 2024.

Google, "European regulations overview and guidance Ad technology providers," https://support.google.com/admanager/answer/9012903. Accessed August 19, 2024.

Google, "OpenRTB Integration," https://developers.google.com/authorized-buyers/rtb/openrtb-guide. Accessed August 19, 2024.

Google, "Process the Request," https://developers.google.com/authorized-buyers/rtb/request-guide. Accessed August 19, 2024.

Google, "Real-time Bidding," https://developers.google.com/authorized-buyers/rtb/start. Accessed August 19, 2024.

Google, "Sign in and sync in Chrome," https://support.google.com/chrome/answer/185277?hl=en&co=GENIE.Platform%3DDesktop. Accessed September 6, 2024.

Greene, D., "As G Suite gains traction in the enterprise, G Suite's Gmail and consumer Gmail to more closely align," https://blog.google/products/gmail/g-suite-gains-traction-in-the-enterprise-g-suites-gmail-and-consumer-gmail-to-more-closely-align/. Accessed September 6, 2024.

Heine, F., "Google changes user data practices to end German antitrust probe," https://www.reuters.com/technology/german-cartel-office-google-users-have-better-control-over-their-data-2023-10-05/. Accessed August 16, 2024.

Jones Harbour, P., "In the matter of Google/DoubleClick F.T.C. File No. 071-0170 Dissenting statement of Commissioner Pamela Jones Harbour," (December 20, 2007) https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf. Accessed August 20, 2024.

Martin, N., "How Much Does Google Really Know About You? A Lot," https://www.forbes.com/sites/nicolemartin1/2019/03/11/how-much-does-google-really-know-about-you-a-lot/. Accessed August 29, 2024.

Oracle Data Cloud, "2019 Data Directory," https://web.archive.org/web/20210420081301/https://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf. Accessed August 19, 2024.

Perry, V., Hoffman, D., "George Talks Business- Donna Hoffman," https://www.youtube.com/watch?v=VVYPfmlUwmg. Accessed on August 8, 2024.

Ron Wyden United States Senator for Oregon, "Wyden Releases Draft Legislation to Protect Americans' Personal Data From Hostile Foreign Governments," https://www.wyden.senate.gov/news/press-releases/wyden-releases-draft-legislation-to-protect-americans-personal-data-from-hostile-foreign-governments. Accessed August 27, 2024.

Ron Wyden United States Senator for Oregon, "Wyden, Bipartisan Senators, Question Online Ad Exchanges on Sharing of Americans' Data with Foreign Companies," (April 02, 2021) https://www.wyden.senate.gov/news/press-releases/wyden-bipartisan-senators-question-online-ad-exchanges-on-sharing-of-americans-data-with-foreign-companies. Accessed August 28, 2024.

StatCounter, "Search Engine Market Share United States of America," https://gs.statcounter.com/search-engine-market-share/all/united-states-of-america. Accessed September 6, 2024.

Statista, "Market share of leading internet browsers in the United States and worldwide as of August 2024," https://www.statista.com/statistics/276738/worldwide-and-us-market-share-of-leading-internet-browsers. Accessed September 5, 2024.

Statista, "Most popular mapping apps in the United States as of April 2018, by reach," https://www.statista.com/statistics/865419/most-popular-us-mapping-apps-ranked-by-reach/. Accessed August 19, 2024.

Stigler Committee on Digital Platforms, "Final Report," (September 2019) https://research.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf?la=en&hash=2D23583FF8BCC560B7FEF7A81E1F95C1DDC5225E. Accessed August 28, 2024.

Sussman et al., "FTC AMICUS CURIAE BRIEF CASE NOS. 3:21-md-02981-JD; 3:20-cv-05671-JD," (August 12, 2024) https://www.ftc.gov/system/files/ftc_gov/pdf/ftc_amicus_brief_epic_v_google_play.pdf. Accessed August 28, 2024.

The Bundeskartellamt, "Decision pursuant to Section 19a(2) sentence 4 in conjunction with Section 32b(1) GWB - Public version," (June 10, 2023) https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2023/B7-70-21.pdf. Accessed August 16, 2024.

The Norwegian Consumer Council, "Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy," (June 27, 2018) https://storage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf. Accessed on August 19, 2024.

Vincent J., "France fines Google and Facebook for pushing tracking cookies on users with dark patterns / One button to accept all — but not to reject all," https://www.theverge.com/2022/1/7/22871719/france-fines-google-facebook-cookies-tracking-dark-patterns-eprivacy. Accessed on August 8, 2024.

VII. APPENDIX B: MATERIALS CONSIDERED

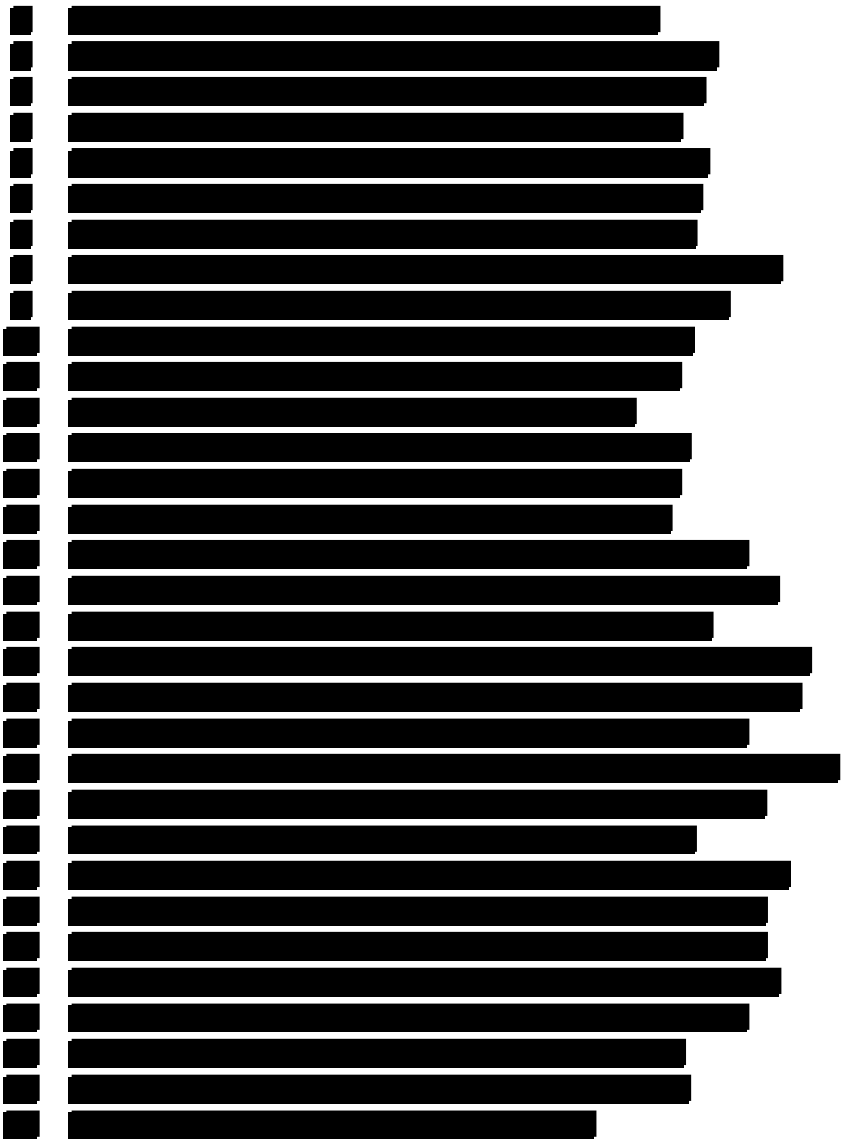
A. Discovery Responses

All available discovery responses produced within the matter of *The State of Texas, et al. v. Google*, Case Number: 4:20-cv-00957-SDJ, including:

1. The Parties' amended initial disclosures;
2. The Parties' discovery responses and objections to Interrogatories, Requests for Admission, and Requests for Production; and
3. Google's written responses to Plaintiffs' Rule 30(b)(6) Notice.

B. Declarations Transcripts & Exhibits

All available deposition transcripts and exhibits within the matter of *The State of Texas, et al. v. Google*, Case Number: 4:20-cv-00957-SDJ, including:



[redacted]

All available deposition transcripts and exhibits within the matter of *USA v. Google*, Case Number: 1:23-cv-00108-LMB-JFA, including:

[redacted]

110. Deposition and Exhibits of Jonathan Bellack (November, 11, 2023)

[redacted]

112. Deposition and Exhibits of K. Marco Hardie (November 14, 2023)
113. Deposition and Exhibits of Jason Hsueh (November 15, 2023)
114. Deposition and Exhibits of Nirmal Jayaram (November 14, 2023)
115. Deposition and Exhibits of Nitish Korula (30B6 errata only) (November 14, 2023)
116. Deposition and Exhibits of Nitish Korula (November 3, 2023)
117. Deposition and Exhibits of Chris LaSala (August 16, 2023)
118. Deposition and Exhibits of Chris LaSala (November 7, 2023)
119. Deposition and Exhibits of Eisar Lipkovitz (November 9, 2023)
120. Deposition and Exhibits of Neal Mohan (October 30, 2023)
121. Deposition and Exhibits of Apama Pappu (August 11, 2023)

122. Deposition and Exhibits of Apama Pappu (November 2, 2023)
123. Deposition and Exhibits of Vladislav Sinaniyev (November 16, 2023)
[redacted]
125. Deposition and Exhibits of Ali Amini (November 14-15, 2023)
126. Deposition and Exhibits of Atil Iscen (April 1, 2024)
127. Deposition and Exhibits of Benjamin Kornacki (November 3, 2024)
128. Deposition and Exhibits of Nitish Korula (November 3, 2024)
129. Deposition and Exhibits of Nitish Korush (30(b)6) (November 14, 2023)
130. Deposition and Exhibits of Chris LaSala (August 16, 2023)
131. Deposition and Exhibits of Chris LaSala (November 7, 2023)
132. Deposition and Exhibits of Eisar Lipkovitz (November 9, 2023)
133. Deposition and Exhibits of Tim Lipus (April 3, 2024)
134. Deposition and Exhibits of Neal Mohan (October 10, 2023 and November 8, 2023)
135. Deposition and Exhibits of Martin Pal (April 17, 2024)
136. Deposition and Exhibits of Bonita Stewart (April 29, 2024)
137. Deposition and Exhibits of Nitish Korula (Noveber 11, 2023)
138. Deposition and Exhibits of Neal Mohan (October 10, 2023)

All available deposition transcripts and exhibits within the matter of *In re: Google Digital Advertising Antitrust Litigation*, Case Number: 1:21-md-03010-PKC, including the depositions and exhibits of:

[redacted]	[redacted]
140.Bergamaschi, Natalia	6/20/2024
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
144.Cox, Sam	6/25/2024
[redacted]	[redacted]
146.Deily, Eric (Google)	7/23/2024
147.Graff, David (Google)	7/23/2024
148.Gringras, Richard	6/18/2024
[redacted]	[redacted]
[redacted]	[redacted]
151.Jankovsky, Brian	7/10/2024
152.Jayaram, Nirmal	4/25/2024
153.Jayaram, Nirmal	7/10/2024
154.Kim, Woojin	6/24/2024
155.Korula, Nitish	7/12/2024
156.LaSalle, James	6/12/2024
157.Levitte, George	6/13/2024
158.Lin, Max	5/2/2024
[redacted]	[redacted]
160.Loubser, Max	6/6/2024
161.May, Stuart (Google)	6/28/2024
[redacted]	[redacted]
163.Pal, Martin	6/4/2024

[redacted]	[redacted]
166.Richter, Peggy	6/25/2024
167.Rowley, Bryan	6/26/2024
168.Sajous, Nathalie	6/10/2024
[redacted]	[redacted]
171.Shellhammer, Alex	6/7/2024
172.Spencer, Scott	6/25/2024
[redacted]	[redacted]
175.Taylor, Dan	6/24/2024
176.Towle, Christina	6/27/2024
[redacted]	[redacted]

Other available deposition transcripts and exhibits, including the depositions and exhibits of:

179.Bellack, Jonathan	10/2/2020
[redacted]	[redacted]
181.Braddi, Joan	7/28/2020
182.Brady, Patrick	7/21/2020
183.Cox, Sam	10/26/2020
184.Giles, Jim	11/6/2020
185.Kolotouros, Jim	7/31/2020
186.Kyncl, Robert	9/25/2020
187.LaSala, Chris	10/20/2020
188.Li,Christopher	7/17/2020
189.Maurer, Tobias	11/9/2020
190.Mohan, Neal	11/19/2020
191.Pimplapure, Ashish	7/24/2020
192.Rosenberg, Jamie	7/14/2020
193.Shodjai, Payam	11/10/2020
194.Weinstein, Debbie	11/2/2020
195.Dischler, Jerry	9/28/2020
196.Dischler, Jerry	2/3/2022
197.Dukellis, John	8/11/2021
198.Dukellis, John	2/28/2022
199.Harrison, Donald	10/19/2021
200.Hsiao, Sissie	12/9/2021
201.Jayaram, Nirmal	9/17/2021
202.Kachachi, Bashar	11/20/2020
203.Kim, Woojin	3/30/2021
204.Korula, Nitish	10/28/2021

[redacted]

C. Pleadings

The live pleadings (complaint and answer) within the matter of The State of Texas, et al. v. Google, Case Number: 4:20-cv-00957-SDJ, including the Fourth Amended Complaint.

D. Expert Reports & Declarations

All available expert reports, including appendices, backup materials, and cited materials, within the matter of *The State of Texas, et al. v. Google*, Case Number: 4:20-cv-00957-SDJ, including:

1. 2024.06.07 Expert Report of Jeffrey S. Andrien
2. 2024.06.07 Expert Report of Joshua Gans, as well as 2024.07.24 Errata and Supplemental Appendix D
3. 2024.06.07 Expert Report of Jacob Hostetler
4. 2024.06.07 Expert Report of John Chandler
5. 2024.06.07 Expert Report of Matthew Weinberg
6. 2024.06.07 Expert Report of Parag Pathak
7. 2024.07.30 Expert Report of Anindya Ghose
8. 2024.07.30 Expert Report of Donna L. Hoffman
9. 2024.07.30 Expert Report of Douglas Skinner
10. 2024.07.30 Expert Report of Itamar Simonson
11. 2024.07.30 Expert Report of Martin C. Rinard
12. 2024.07.30 Expert Report of Paul R. Milgrom
13. 2024.07.30 Expert Report of Steven N. Wiggins
14. 2024.08.06 Expert Report of Michael R. Baye
15. 2024.08.06 Expert Report of Jason Nieh

All available expert reports (with redactions) within the matter of *USA v. Google*, Case Number: 1:23-cv-00108-LMB-JFA, including:

1. Declarations of Google Employees
2. 2023.12.22 Expert Report of Gabriel Weintraub, GOOG-AT-MDL-C-000018734
3. 2023.12.22 Expert Report of R. Ravi, GOOG-AT-MDL-C-000019017

4. 2023.12.22 Expert Report of Robin S. Lee, GOOG-AT-MDL-C-000019273
5. 2023.12.22 Expert Report of Rosa Abrantes-Metz, GOOG-AT-MDL-C-000019786
6. 2023.12.22 Expert Report of Thomas S. Respess, GOOG-AT-MDL-C-000020106
7. 2023.12.22 Expert Report of Timothy Simcoe, GOOG-AT-MDL-C-000020274
8. 2024.01.13 Errata to Abrantes-Metz Expert Report, GOOG-AT-MDL-C-000020435
9. 2024.01.13 Errata to Ravi Expert Report, GOOG-AT-MDL-C-000020437
10. 2024.01.13 Errata to Respess Expert Report, GOOG-AT-MDL-C-000020440
11. 2024.01.13 Errata to Simcoe Expert Report, GOOG-AT-MDL-C-000020467
12. 2024.01.13 Errata to Weintraub Expert Report, GOOG-AT-MDL-C-000020471
13. 2024.01.23 Chevalier Expert Report, GOOG-AT-MDL-C-000020474
14. 2024.01.23 Ferrante Expert Report, GOOG-AT-MDL-C-000020714
15. 2024.01.23 Ghose Expert Report, GOOG-AT-MDL-C-000020767
16. 2024.01.23 Israel Expert Report, GOOG-AT-MDL-C-000021036
17. 2024.01.23 Milgrom Expert Report, GOOG-AT-MDL-C-000021794
18. 2024.01.23 Rinard Expert Report, GOOG-AT-MDL-C-000022191
19. 2024.01.23 Shirky Expert Report, GOOG-AT-MDL-C-000022229
20. 2024.01.23 Simonson Expert Report, GOOG-AT-MDL-C-000022290
21. 2024.01.23 Skinner Expert Report, GOOG-AT-MDL-C-000022948
22. 2024.02.13 Expert Rebuttal Report of Adoria Lim, GOOG-AT-MDL-C-000023002
23. 2024.02.13 Expert Rebuttal Report of Gabriel Weintraub, GOOG-AT-MDL-C-000023226
24. 2024.02.13 Expert Rebuttal Report of Kenneth Wilbur, GOOG-AT-MDL-C-000023322
25. 2024.02.13 Expert Rebuttal Report of R. Ravi, GOOG-AT-MDL-C-000023435
26. 2024.02.13 Expert Rebuttal Report of Robin S. Lee, GOOG-AT-MDL-C-000023516
27. 2024.02.13 Expert Rebuttal Report of Rosa Abrantes-Metz, GOOG-AT-MDL-C-000023887
28. 2024.02.13 Expert Rebuttal Report of Timothy Simcoe, GOOG-AT-MDL-C-000024064
29. 2024.02.13 Expert Rebuttal Report of Wayne Hoyer, GOOG-AT-MDL-C-000024138
30. 2024.02.13 Expert Rebuttal Report of Wenke Lee, GOOG-AT-MDL-C-000024270
31. 2024.02.16 Errata to Ravi Rebuttal Report, GOOG-AT-MDL-C-000024387
32. 2024.02.20 Errata to Simcoe Rebuttal Report, GOOG-AT-MDL-C-000024389
33. 2024.02.23 Errata to Weintraub Rebuttal Report, GOOG-AT-MDL-C-000024390
34. 2024.02.23 Supplemental Errata to Weintraub Expert Report, GOOG-AT-MDL-C-000024391
35. 2024.02.24 Errata to Wilbur Rebuttal Report, GOOG-AT-MDL-C-000024392
36. 2024.02.26 Errata to Hoyer Rebuttal Report, GOOG-AT-MDL-C-000024397
37. 2024.02.28 Errata to Abrantes-Metz Rebuttal Report, GOOG-AT-MDL-C-000024399
38. 2024.03.04 Expert Supplemental Report of Robin S. Lee, GOOG-AT-MDL-C-000024403
39. 2024.03.08 Consolidated Errata to Lee Rebuttal Report, GOOG-AT-MDL-C-000024436
40. 2024.01.13 Expert Report of Weintraub Errata, GOOG-AT-MDL-C-000040965
41. 2024.01.13 Expert Report of Simcoe Errata, GOOG-AT-MDL-C-000040961

42. 2024.01.13 Expert Report of Respess Errata_with Figure Errata_Redacted, GOOG-AT-MDL-C-000040934
43. 2024.01.13 Expert Report of R Ravi Errata, GOOG-AT-MDL-C-000040931
44. 2024.01.13 Expert Report of Abrantes-Metz Errata, GOOG-AT-MDL-C-000040929
45. 2024.03.08 Consolidated Errata to Lee Rebuttal Report, GOOG-AT-MDL-C-000040926
46. 2024.03.04 Expert Supplemental Report of Robin S. Lee, PhD, GOOG-AT-MDL-C-000040893
47. 2024.02.28 Rebuttal Report Errata of Rosa Abrantes-Metz Signed, GOOG-AT-MDL-C-000040889
48. 2024.02.25 Expert Rebuttal Report of Hoyer Errata, GOOG-AT-MDL-C-000040887
49. 2024.02.24 Wilbur Rebuttal Errata, GOOG-AT-MDL-C-000040882
50. 2024.02.23 Weintraub Rebuttal Report Errata, GOOG-AT-MDL-C-000040881
51. 2024.02.23 Expert Report of Weintraub Supplemental Errata, GOOG-AT-MDL-C-000040880
52. 2024.02.20 Errata to Simcoe Rebuttal Report, GOOG-AT-MDL-C-000040879
53. 2024.02.16 Errata to Ravi Rebuttal Report (Highly Confidential), GOOG-AT-MDL-C-000040877
54. 2024.02.13 Rebuttal Report of Rosa Abrantes-Metz, GOOG-AT-MDL-C-000040700
55. 2024.02.13 Expert Report of Wenke Lee, GOOG-AT-MDL-C-000040583
56. 2024.02.13 Expert Rebuttal Report of Wayne Hoyer, GOOG-AT-MDL-C-000040451
57. 2024.02.13 Expert Rebuttal Report of Timothy Simcoe_Redacted, GOOG-AT-MDL-C-000040377
58. 2024.02.13 Expert Rebuttal Report of Robin S. Lee_Redacted, GOOG-AT-MDL-C-000040006
59. 2024.02.13 Expert Rebuttal Report of R Ravi, GOOG-AT-MDL-C-000039925
60. 2024.02.13 Expert Rebuttal Report of Kenneth Wilbur_Redacted, GOOG-AT-MDL-C-000039812
61. 2024.02.13 Expert Rebuttal Report of Gabriel Weintraub_Redacted, GOOG-AT-MDL-C-000039716
62. 2024.02.13 Expert Rebuttal Report of Adoria Lim_Redacted, GOOG-AT-MDL-C-000039492
63. 2024.01.23 Expert Report of William Clay Shirky, GOOG-AT-MDL-C-000039431
64. 2024.01.23 Expert Report of Paul R. Milgrom, GOOG-AT-MDL-C-000039034
65. 2024.01.23 Expert Report of Martin C. Rinard, GOOG-AT-MDL-C-000038996
66. 2024.01.23 Expert Report of Mark A. Israel_Redacted, GOOG-AT-MDL-C-000038238
67. 2024.01.23 Expert Report of Judith A. Chevalier_Redacted, GOOG-AT-MDL-C-000037998
68. 2024.01.23 Expert Report of Itamar Simonson, GOOG-AT-MDL-C-000037340
69. 2024.01.23 Expert Report of Douglas Skinner, GOOG-AT-MDL-C-000037286
70. 2024.01.23 Expert Report of Anthony J. Ferrante, GOOG-AT-MDL-C-000037233
71. 2024.01.23 Expert Report of Anindya Ghose_Redacted, GOOG-AT-MDL-C-000036954
72. 2023.12.22 Expert Report of Timothy Simcoe_Redacted, GOOG-AT-MDL-C-000036793
73. 2023.12.22 Expert Report of Thomas Respess_Redacted, GOOG-AT-MDL-C-000036625
74. 2023.12.22 Expert Report of Rosa Abrantes-Metz_Redacted, GOOG-AT-MDL-C-000036305
75. 2023.12.22 Expert Report of Robin S. Lee, PhD_Redacted, GOOG-AT-MDL-C-000035792
76. 2023.12.22 Expert Report of R Ravi_Redacted, GOOG-AT-MDL-C-000035536
77. 2023.12.22 Expert Report of Gabriel Weintraub_Redacted, GOOG-AT-MDL-C-000035253

E. Documents from Production

Bates Stamped Productions, including access to Plaintiffs' entire production database, as well as the following documents and Google and third-party productions made since June 7, 2024:

[redacted]
GOOG-AT-MDL-000992253
GOOG-AT-MDL-000993528
GOOG-AT-MDL-001004706
GOOG-AT-MDL-001055011
GOOG-AT-MDL-001079596
GOOG-AT-MDL-001263607
GOOG-AT-MDL-001390405
GOOG-AT-MDL-001390730
GOOG-AT-MDL-001391213
GOOG-AT-MDL-001392701
GOOG-AT-MDL-001393488
GOOG-AT-MDL-001401594
GOOG-AT-MDL-001414841
GOOG-AT-MDL-001482046
GOOG-AT-MDL-001827568
GOOG-AT-MDL-001933227
GOOG-AT-MDL-001950737
GOOG-AT-MDL-002025788
GOOG-AT-MDL-002034479
GOOG-AT-MDL-002039510
GOOG-AT-MDL-002105969
GOOG-AT-MDL-002105984
GOOG-AT-MDL-002124829
GOOG-AT-MDL-002255894
GOOG-AT-MDL-002273709
GOOG-AT-MDL-002390899
GOOG-AT-MDL-002393442
GOOG-AT-MDL-002424535
GOOG-AT-MDL-003132627
GOOG-AT-MDL-003161451
GOOG-AT-MDL-003216638
GOOG-AT-MDL-003926004
GOOG-AT-MDL-003982416
GOOG-AT-MDL-004074544
GOOG-AT-MDL-004232880
GOOG-AT-MDL-004233138
GOOG-AT-MDL-004291092
GOOG-AT-MDL-004300268
GOOG-AT-MDL-004416785
GOOG-AT-MDL-004436768
GOOG-AT-MDL-004523197
GOOG-AT-MDL-004555181
GOOG-AT-MDL-004605709
GOOG-AT-MDL-004608663

GOOG-AT-MDL-005917323
GOOG-AT-MDL-006062681
GOOG-AT-MDL-006066600
GOOG-AT-MDL-006066635
GOOG-AT-MDL-006066709
GOOG-AT-MDL-006067042
GOOG-AT-MDL-006099844
GOOG-AT-MDL-006100332
GOOG-AT-MDL-006114057
GOOG-AT-MDL-006114190
GOOG-AT-MDL-006115306
GOOG-AT-MDL-006161050
GOOG-AT-MDL-006199360
GOOG-AT-MDL-006214742
GOOG-AT-MDL-006217592
GOOG-AT-MDL-006334729
GOOG-AT-MDL-006466049
GOOG-AT-MDL-006545758
GOOG-AT-MDL-006553324
GOOG-AT-MDL-006554061
GOOG-AT-MDL-006577895
GOOG-AT-MDL-006687067
GOOG-AT-MDL-006759431
GOOG-AT-MDL-006776795
GOOG-AT-MDL-006810972
GOOG-AT-MDL-006873424
GOOG-AT-MDL-006896591
GOOG-AT-MDL-006966530
GOOG-AT-MDL-007175167
GOOG-AT-MDL-007199388
GOOG-AT-MDL-007209980
GOOG-AT-MDL-007213604
GOOG-AT-MDL-007227261
GOOG-AT-MDL-007233150
GOOG-AT-MDL-007236450
GOOG-AT-MDL-007320028
GOOG-AT-MDL-007343585
GOOG-AT-MDL-007346556
GOOG-AT-MDL-007364833
GOOG-AT-MDL-007375672
GOOG-AT-MDL-007387750
GOOG-AT-MDL-007397182
GOOG-AT-MDL-007397197
GOOG-AT-MDL-007418936
GOOG-AT-MDL-007418936
GOOG-AT-MDL-007460868
GOOG-AT-MDL-007920518
GOOG-AT-MDL-007921060
GOOG-AT-MDL-008148533 / GOOG-AT-MDL-008148529
GOOG-AT-MDL-008517788
GOOG-AT-MDL-008588684
GOOG-AT-MDL-008607170
GOOG-AT-MDL-008682082 / GOOG-AT-MDL-008682071
GOOG-AT-MDL-008754374
GOOG-AT-MDL-008835346
GOOG-AT-MDL-008858602
GOOG-AT-MDL-008859799
GOOG-AT-MDL-008881206
GOOG-AT-MDL-008886980
GOOG-AT-MDL-008953893
GOOG-AT-MDL-008964888
GOOG-AT-MDL-008979664
GOOG-AT-MDL-008991390
GOOG-AT-MDL-009012241
GOOG-AT-MDL-009026140
GOOG-AT-MDL-009038893
GOOG-AT-MDL-009289718
GOOG-AT-MDL-009291120
GOOG-AT-MDL-009299907
GOOG-AT-MDL-009321580
GOOG-AT-MDL-009429957
GOOG-AT-MDL-009695495
GOOG-AT-MDL-012335682
GOOG-AT-MDL-012512067
GOOG-AT-MDL-012514705
GOOG-AT-MDL-012524006
GOOG-AT-MDL-012549335
GOOG-AT-MDL-012564903
GOOG-AT-MDL-012693796
GOOG-AT-MDL-012760228
GOOG-AT-MDL-012767138
GOOG-AT-MDL-012809293
GOOG-AT-MDL-012820040
GOOG-AT-MDL-012837016
GOOG-AT-MDL-012857198
GOOG-AT-MDL-012933520
GOOG-AT-MDL-013162482
GOOG-AT-MDL-013290688

GOOG-AT-MDL-013291089
GOOG-AT-MDL-013292974
GOOG-AT-MDL-013299524
GOOG-AT-MDL-013299531
GOOG-AT-MDL-013300202
GOOG-AT-MDL-013378392
GOOG-AT-MDL-013663380
GOOG-AT-MDL-013745210
GOOG-AT-MDL-013785243
GOOG-AT-MDL-013803908
GOOG-AT-MDL-013908958
GOOG-AT-MDL-013918668
GOOG-AT-MDL-014224279
GOOG-AT-MDL-014399819
GOOG-AT-MDL-014427012
GOOG-AT-MDL-014460206
GOOG-AT-MDL-014462378
GOOG-AT-MDL-014486274
GOOG-AT-MDL-014524447
GOOG-AT-MDL-014618288
GOOG-AT-MDL-015084038
GOOG-AT-MDL-015241235
GOOG-AT-MDL-015436738
GOOG-AT-MDL-015622194
GOOG-AT-MDL-015642731
GOOG-AT-MDL-015644231
GOOG-AT-MDL-015844174
GOOG-AT-MDL-015929587
GOOG-AT-MDL-015997353
GOOG-AT-MDL-016042614
GOOG-AT-MDL-016354429
GOOG-AT-MDL-016365471
GOOG-AT-MDL-016443713
GOOG-AT-MDL-016448141
GOOG-AT-MDL-016457027
GOOG-AT-MDL-016471362
GOOG-AT-MDL-016478947
GOOG-AT-MDL-016534880
GOOG-AT-MDL-016627159
GOOG-AT-MDL-016635166
GOOG-AT-MDL-016636451
GOOG-AT-MDL-016639543
GOOG-AT-MDL-016641375
GOOG-AT-MDL-016641386
GOOG-AT-MDL-016644492
GOOG-AT-MDL-016647207
GOOG-AT-MDL-016656237
GOOG-AT-MDL-016659168
GOOG-AT-MDL-016679999
GOOG-AT-MDL-016756296
GOOG-AT-MDL-016772599
GOOG-AT-MDL-016786406
GOOG-AT-MDL-016838311
GOOG-AT-MDL-016851808
GOOG-AT-MDL-016924839
GOOG-AT-MDL-016937590
GOOG-AT-MDL-016943922
GOOG-AT-MDL-016967094
GOOG-AT-MDL-017132714
GOOG-AT-MDL-017182526
GOOG-AT-MDL-017186637
GOOG-AT-MDL-017187837
GOOG-AT-MDL-017200359
GOOG-AT-MDL-017201432
GOOG-AT-MDL-017295265
GOOG-AT-MDL-017394050
GOOG-AT-MDL-017431476
GOOG-AT-MDL-017489022
GOOG-AT-MDL-017494582
GOOG-AT-MDL-017599092
GOOG-AT-MDL-017664768
GOOG-AT-MDL-017746412
GOOG-AT-MDL-017749638
GOOG-AT-MDL-017762649
GOOG-AT-MDL-017815242
GOOG-AT-MDL-017864022
GOOG-AT-MDL-018248228
GOOG-AT-MDL-018342853
GOOG-AT-MDL-018411861
GOOG-AT-MDL-018427318
GOOG-AT-MDL-018448707
GOOG-AT-MDL-018548592
GOOG-AT-MDL-018618351
GOOG-AT-MDL-018639511
GOOG-AT-MDL-018652651
GOOG-AT-MDL-018791825
GOOG-AT-MDL-018798202
GOOG-AT-MDL-018798325
GOOG-AT-MDL-018801438
GOOG-AT-MDL-018810983

GOOG-AT-MDL-018840626
GOOG-AT-MDL-018998910
GOOG-AT-MDL-019001498
GOOG-AT-MDL-019120021
GOOG-AT-MDL-019138917
GOOG-AT-MDL-019150053
GOOG-AT-MDL-019206323
GOOG-AT-MDL-019236572
GOOG-AT-MDL-019236942
GOOG-AT-MDL-019246913
GOOG-AT-MDL-019300501
GOOG-AT-MDL-019306356
GOOG-AT-MDL-019325621
GOOG-AT-MDL-019354485
GOOG-AT-MDL-019376191
GOOG-AT-MDL-019386250
GOOG-AT-MDL-019521557
GOOG-AT-MDL-019538278
GOOG-AT-MDL-019543895
GOOG-AT-MDL-019552139
GOOG-AT-MDL-019571201
GOOG-AT-MDL-019583234
GOOG-AT-MDL-019583793
GOOG-AT-MDL-019588187
GOOG-AT-MDL-019633443
GOOG-AT-MDL-019642313
GOOG-AT-MDL-019653406
GOOG-AT-MDL-019674484
GOOG-AT-MDL-019708452
GOOG-AT-MDL-019709036
GOOG-AT-MDL-019721340
GOOG-AT-MDL-019767203
GOOG-AT-MDL-019782935
GOOG-AT-MDL-B-000134141
GOOG-AT-MDL-B-000883782
GOOG-AT-MDL-B-001084151
GOOG-AT-MDL-B-001140202
GOOG-AT-MDL-B-002087955
GOOG-AT-MDL-B-002088697
GOOG-AT-MDL-B-002088752
GOOG-AT-MDL-B-002088926
GOOG-AT-MDL-B-002090567
GOOG-AT-MDL-B-002091565
GOOG-AT-MDL-B-002095353
GOOG-AT-MDL-B-002095501
GOOG-AT-MDL-B-002095769
GOOG-AT-MDL-B-002097533
GOOG-AT-MDL-B-002097570
GOOG-AT-MDL-B-002097648
GOOG-AT-MDL-B-002098265
GOOG-AT-MDL-B-002099366
GOOG-AT-MDL-B-002105135
GOOG-AT-MDL-B-002500395
GOOG-AT-MDL-B-002514153
GOOG-AT-MDL-B-002547489
GOOG-AT-MDL-B-002552122
GOOG-AT-MDL-B-002624643
GOOG-AT-MDL-B-002760309
GOOG-AT-MDL-B-002762758
GOOG-AT-MDL-B-002763194
GOOG-AT-MDL-B-002764178
GOOG-AT-MDL-B-002764191
GOOG-AT-MDL-B-002797051
GOOG-AT-MDL-B-002803919
GOOG-AT-MDL-B-002837096
GOOG-AT-MDL-B-003181628
GOOG-AT-MDL-B-003735823
GOOG-AT-MDL-B-003741154
GOOG-AT-MDL-B-004008753
GOOG-AT-MDL-B-004015880
GOOG-AT-MDL-B-004016318
GOOG-AT-MDL-B-004243337
GOOG-AT-MDL-B-004247242
GOOG-AT-MDL-B-004265772
GOOG-AT-MDL-B-004356180
GOOG-AT-MDL-B-004425247
GOOG-AT-MDL-B-004438679
GOOG-AT-MDL-B-004680051
GOOG-AT-MDL-B-005083974
GOOG-AT-MDL-B-005167304
GOOG-AT-MDL-B-005168118
GOOG-AT-MDL-B-005170475
GOOG-AT-MDL-B-005180695
GOOG-AT-MDL-B-005180787
GOOG-AT-MDL-B-005282318
GOOG-AT-MDL-B-005372599
GOOG-AT-MDL-B-005457387
GOOG-AT-MDL-B-006069467
GOOG-AT-MDL-B-006122575
GOOG-AT-MDL-B-006146533

GOOG-AT-MDL-B-006316352
GOOG-AT-MDL-B-006365895
GOOG-AT-MDL-B-006365981
GOOG-AT-MDL-B-006651543
GOOG-AT-MDL-B-006666952
GOOG-AT-MDL-B-006939056
GOOG-AT-MDL-B-007212533
GOOG-AT-MDL-B-007229334
GOOG-AT-MDL-B-007232867
GOOG-AT-MDL-B-007353902
GOOG-AT-MDL-B-007717215
GOOG-DOJ-12948968
GOOG-DOJ-13897780
GOOG-DOJ-13899823
GOOG-DOJ-13911836
GOOG-DOJ-13930748
GOOG-DOJ-13940086
GOOG-DOJ-14008698
GOOG-DOJ-14010783
GOOG-DOJ-14034714
GOOG-DOJ-14113270
GOOG-DOJ-14139857
GOOG-DOJ-14155066
GOOG-DOJ-14156827
GOOG-DOJ-14161619
GOOG-DOJ-14161943
GOOG-DOJ-14232497
GOOG-DOJ-14352302
GOOG-DOJ-14352774
GOOG-DOJ-14365517
GOOG-DOJ-14433486
GOOG-DOJ-14433633
GOOG-DOJ-14435110
GOOG-DOJ-14436029
GOOG-DOJ-14453674
GOOG-DOJ-14458088
GOOG-DOJ-14494204
GOOG-DOJ-14544715
GOOG-DOJ-14544743
GOOG-DOJ-14556699
GOOG-DOJ-14639213
GOOG-DOJ-14712739
GOOG-DOJ-14717683
GOOG-DOJ-14733660
GOOG-DOJ-14735212
GOOG-DOJ-14735427
GOOG-DOJ-14740782
GOOG-DOJ-14743636
GOOG-DOJ-14870370
GOOG-DOJ-15021111
GOOG-DOJ-15022600
GOOG-DOJ-15022611
GOOG-DOJ-15029681
GOOG-DOJ-15041717
GOOG-DOJ-15042589
GOOG-DOJ-15064786
GOOG-DOJ-15071642
GOOG-DOJ-15073261
GOOG-DOJ-15076754
GOOG-DOJ-15140608
GOOG-DOJ-15173140
GOOG-DOJ-15186471
GOOG-DOJ-15278949
GOOG-DOJ-15371972
GOOG-DOJ-15417170
GOOG-DOJ-15426837
GOOG-DOJ-15427800
GOOG-DOJ-15428154
GOOG-DOJ-15432090
GOOG-DOJ-15433127
GOOG-DOJ-15434544
GOOG-DOJ-15445478
GOOG-DOJ-15526215
GOOG-DOJ-15590044
GOOG-DOJ-15595543
GOOG-DOJ-15597407
GOOG-DOJ-15598151
GOOG-DOJ-15601229
GOOG-DOJ-15616526
GOOG-DOJ-15621021
GOOG-DOJ-15628088
GOOG-DOJ-15631978
GOOG-DOJ-15637110
GOOG-DOJ-15675958
GOOG-DOJ-15703667
GOOG-DOJ-15733030
GOOG-DOJ-15766965
GOOG-DOJ-15789579
GOOG-DOJ-16271009
GOOG-DOJ-16732920

GOOG-DOJ-16976651
GOOG-DOJ-17101302
GOOG-DOJ-17105055
GOOG-DOJ-17581278
GOOG-DOJ-17684923
GOOG-DOJ-19090482
GOOG-DOJ-19119112
GOOG-DOJ-24099550
GOOG-DOJ-27760500_DUP_1
GOOG-DOJ-27762649
GOOG-DOJ-27762691
GOOG-DOJ-27796586
GOOG-DOJ-27803156
GOOG-DOJ-27803505
GOOG-DOJ-27803533
GOOG-DOJ-27804205
GOOG-DOJ-27804876
GOOG-DOJ-28244476
GOOG-DOJ-28251977
GOOG-DOJ-28385887
GOOG-DOJ-28420330
GOOG-DOJ-28441892
GOOG-DOJ-28485979
GOOG-DOJ-29373435
GOOG-DOJ-29427368
GOOG-DOJ-29453844
GOOG-DOJ-30066802
GOOG-DOJ-32018179
GOOG-DOJ-32018452
GOOG-DOJ-32022422
GOOG-DOJ-32062262
GOOG-DOJ-32262980
GOOG-DOJ-32265694
GOOG-DOJ-32312862
GOOG-DOJ-32330679
GOOG-DOJ-AT-00003565
GOOG-DOJ-AT-00087809
GOOG-DOJ-AT-00193219
GOOG-DOJ-AT-00193564
GOOG-DOJ-AT-00252559
GOOG-DOJ-AT-00504048
GOOG-DOJ-AT-00569953
GOOG-DOJ-AT-00575435
GOOG-DOJ-AT-00585351
GOOG-DOJ-AT-00588995
GOOG-DOJ-AT-00651561
GOOG-DOJ-AT-00663174
GOOG-DOJ-AT-00750354
GOOG-DOJ-AT-01019411
GOOG-DOJ-AT-01027937
GOOG-DOJ-AT-01029300
GOOG-DOJ-AT-01033235
GOOG-DOJ-AT-01101118
GOOG-DOJ-AT-01151260
GOOG-DOJ-AT-01514374
GOOG-DOJ-AT-01525829
GOOG-DOJ-AT-01682499
GOOG-DOJ-AT-01688915
GOOG-DOJ-AT-01811246
GOOG-DOJ-AT-01814428
GOOG-DOJ-AT-01814688
GOOG-DOJ-AT-01815482
GOOG-DOJ-AT-01816686
GOOG-DOJ-AT-01848255
GOOG-DOJ-AT-01933085
GOOG-DOJ-AT-02070545
GOOG-DOJ-AT-02122748
GOOG-DOJ-AT-02146896
GOOG-DOJ-AT-02153612
GOOG-DOJ-AT-02193427
GOOG-DOJ-AT-02198297
GOOG-DOJ-AT-02230210
GOOG-DOJ-AT-02245345
GOOG-DOJ-AT-02273573
GOOG-DOJ-AT-02273588
GOOG-DOJ-AT-02275074
GOOG-DOJ-AT-02275933
GOOG-DOJ-AT-02298467
GOOG-DOJ-AT-02319393
GOOG-DOJ-AT-02396376
GOOG-DOJ-AT-02443073
GOOG-DOJ-AT-02468512
GOOG-DOJ-AT-02482767
GOOG-DOJ-AT-02509551
GOOG-DOJ-AT-02605782
GOOG-DOJ-AT-02630103
GOOG-DOJ-AT-02634336
GOOG-DOJ-AT-02639830
GOOG-NE-01787563
GOOG-NE-02557667

GOOG-NE-02558055
GOOG-NE-03231727
GOOG-NE-03236272
GOOG-NE-03465199
GOOG-NE-03467508
GOOG-NE-03616222
GOOG-NE-03627597
GOOG-NE-03727939
GOOG-NE-03844060
GOOG-NE-03869994
GOOG-NE-03872605
GOOG-NE-04304005
GOOG-NE-04599495
GOOG-NE-04689402
GOOG-NE-05241137
GOOG-NE-05270679
GOOG-NE-06113062
GOOG-NE-06547825
GOOG-NE-06568562
GOOG-NE-06568719
GOOG-NE-06729717
GOOG-NE-06841582
GOOG-NE-06879032
GOOG-NE-06879156
GOOG-NE-07260811
GOOG-NE-07281619
GOOG-NE-07825865
GOOG-NE-07841238
GOOG-NE-07946731
GOOG-NE-08112779
GOOG-NE-08116078
GOOG-NE-09021813
GOOG-NE-09138394
GOOG-NE-09685424
GOOG-NE-09698556
GOOG-NE-09711564
GOOG-NE-10420747
GOOG-NE-10573952
GOOG-NE-10660658
GOOG-NE-10660882
GOOG-NE-10711686
GOOG-NE-10777158
GOOG-NE-10944631
GOOG-NE-10951113
GOOG-NE-10952313
GOOG-NE-10976657
GOOG-NE-10977717
GOOG-NE-10978402
GOOG-NE-10985565
GOOG-NE-11433745
GOOG-NE-11813912
GOOG-NE-11847370
GOOG-NE-11877282
GOOG-NE-12727978
GOOG-NE-12738745
GOOG-NE-12742008
GOOG-NE-12787759
GOOG-NE-12793239
GOOG-NE-12794242
GOOG-NE-12885078
GOOG-NE-12891184
GOOG-NE-13004102
GOOG-NE-13200100
GOOG-NE-13205235
GOOG-NE-13205865
GOOG-NE-13210272
GOOG-NE-13234204
GOOG-NE-13327192
GOOG-NE-13340752
GOOG-NE-13349343
GOOG-NE-13367768
GOOG-NE-13369624
GOOG-NE-13373170
GOOG-NE-13374150
GOOG-NE-13379438
GOOG-NE-13386334
GOOG-NE-13389481
GOOG-NE-13390045
GOOG-NE-13393115
GOOG-NE-13401911
GOOG-NE-13405025
GOOG-NE-13415537
GOOG-NE-13511239
GOOG-NE-13515136
GOOG-NE-13541543
GOOG-NE-13569193
GOOG-NE-13577462
GOOG-NE-13589899
GOOG-NE-13614917
GOOG-NE-13624783

GOOG-NE-13626680
GOOG-TEX-00001418
GOOG-TEX-00039266
GOOG-TEX-00079344
GOOG-TEX-00089835
GOOG-TEX-00090151
GOOG-TEX-00090282
GOOG-TEX-00090969
GOOG-TEX-00092657
GOOG-TEX-00105202
GOOG-TEX-00105361
GOOG-TEX-00106255
GOOG-TEX-00109167
GOOG-TEX-00110068
GOOG-TEX-00110540
GOOG-TEX-00110544
GOOG-TEX-00111494
GOOG-TEX-00116069
GOOG-TEX-00116639
GOOG-TEX-00119737
GOOG-TEX-00119845
GOOG-TEX-00120626
GOOG-TEX-00120775
GOOG-TEX-00124296
GOOG-TEX-00156142
GOOG-TEX-00167119
GOOG-TEX-00177559
GOOG-TEX-00206687
GOOG-TEX-00216163
GOOG-TEX-00234150
GOOG-TEX-00240572
GOOG-TEX-00270127
GOOG-TEX-00271177
GOOG-TEX-00309326
GOOG-TEX-00326649
GOOG-TEX-00336527
GOOG-TEX-01244428
GOOG-TEX-01279945
GOOG-TEX-00344083
GOOG-TEX-00370306
GOOG-TEX-00374779
GOOG-TEX-00375239
GOOG-TEX-00452866
GOOG-TEX-00453431
GOOG-TEX-00513684
GOOG-TEX-00597317
GOOG-TEX-00643890
GOOG-TEX-00656701
GOOG-TEX-00660928
GOOG-TEX-00689539
GOOG-TEX-00705131
GOOG-TEX-00715805
GOOG-TEX-00716782
GOOG-TEX-00777573
GOOG-TEX-00778301
GOOG-TEX-00797340
GOOG-TEX-00806640
GOOG-TEX-00806682
GOOG-TEX-00814407
GOOG-TEX-00825713
GOOG-TEX-00828547
GOOG-TEX-00831660
GOOG-TEX-00850729
GOOG-TEX-00858576
GOOG-TEX-00905673
GOOG-TEX-00959457
GOOG-TEX-00959461
GOOG-TEX-00969525
GOOG-TEX-00974499
GOOG-TEX-00978814
GOOG-TEX-01004466
GOOG-TEX-01036150
GOOG-TEX-01142635
GOOG-TEX-01155492
[redacted]
[redacted]

F. Books and Papers

Bashir, M. A., Wilson, C. (2018). "Diffusion of User Tracking Data in the Online Advertising Ecosystem." In Proceedings on Privacy Enhancing Technologies, Volume 2018, Issue 4, pp 85-103. DOI: https://doi.org/10.1515/popets-2018-0033

Berke, A., Calacci, D. (2022). "Privacy Limitations of Interest-based Advertising on The Web: A Post-mortem Empirical Analysis of Google's FLoC." CCS '22: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, pp 337 – 349. DOI: https://doi.org/10.1145/3548606.3560626

Beugin, Y., McDaniel, P. (2023). "Interest-disclosing Mechanisms for Advertising are Privacy-Exposing (not Preserving)." In Proceedings on Privacy Enhancing Technologies Symposium (PoPETS) 2024. DOI: https://doi.org/10.48550/arXiv.2306.03825

Beugin, Y., McDaniel, P. (2024). "A Public and Reproducible Assessment of the Topics API on Real Data." SecWeb 2024: Workshop on Designing Security for the Web. DOI: https://doi.org/10.48550/arXiv.2403.19577

Binns R., et al. (2018). "Third Party Tracking in the Mobile Ecosystem". In Proceedings of the 10th ACM Conference on Web Science (WebSci '18). DOI: https://doi.org/10.1145/3201064.3201089

Binns, R., Bietti, E. (2020). "Dissolving privacy, one merger at a time: Competition, data and third party tracking." Computer Law & Security Review, Volume 36. DOI: https://doi.org/10.1016/j.clsr.2019.105369

Carey et al. (2023). "Measuring re-identification risk." In Proceedings of the ACM on Management of Data, pp.1-26. DOI: https://doi.org/10.48550/arXiv.2304.07210

Chen et al. (2021). "Cookie Swap Party: Abusing First-Party Cookies for Web Tracking." WWW '21: Proceedings of the Web Conference 2021. DOI: https://doi.org/10.1145/3442381.3449837

Cook et al. (2019). "Inferring tracker-advertiser relationships in the online advertising ecosystem using header bidding." *arXiv* DOI: https://doi.org/10.48550/arXiv.1907.07275

Dambra et al. (2022). "When Sally Met Trackers: Web Tracking From the Users' Perspective." In the 31st USENIX Security Symposium (USENIX Security 22). https://www.usenix.org/conference/usenixsecurity22/presentation/dambra

Englehardt, S., Narayanan, A. (2016). "Online Tracking: A 1-million-site Measurement and Analysis." In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). DOI: https://doi.org/10.1145/2976749.2978313

Farke et al. (2021). "Are Privacy Dashboards Good for End Users? Evaluating User Perceptions and Reactions to Google's My Activity." In Proceedings of the 30th USENIX Security Symposium. https://www.usenix.org/system/files/sec21-farke.pdf

Gómez-Boix et al. (2018). "Hiding in the Crowd: an Analysis of the Effectiveness of Browser Fingerprinting at Large Scale." In WWW 2018: The 2018 Web Conference. DOI: https://doi.org/10.1145/3178876.3186097

Gray et al. (2018). "The Dark (Patterns) Side of UX Design." In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18). https://doi.org/10.1145/3173574.3174108

Gray et al. (2023). "Towards a Preliminary Ontology of Dark Patterns Knowledge." In Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA '23. DOI: https://doi.org/10.1145/3544549.3585676

Gunawan et al. (2021). "A Comparative Study of Dark Patterns Across Mobile and Web Modalities." In Proceedings of the ACM on Human-Computer Interaction, Volume 5, Issue CSCW2, Article 377, pp 1-29. DOI: https://doi.org/10.1145/3479521

Iqbal et al. (2023). "Tracking, profiling, and ad targeting in the Alexa echo smart speaker ecosystem." In *Proceedings of the 2023 ACM on Internet Measurement Conference*, pp 569-583. DOI: https://doi.org/10.48550/arXiv.2204.10920

Jha et al. (2023). "On the Robustness of Topics API to a Re-Identification Attack". Privacy Enhancing Technologies Symposium (PETS) 2023. DOI: https://doi.org/10.48550/arXiv.2306.05094

Libert, T. (2015). "Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites." In the International Journal of Communication, Volume 9, pp 3544-3561. https://ijoc.org/index.php/ijoc/article/view/3646/1503

Mathur et al. (2021). "What Makes a Dark Pattern... Dark?: Design Attributes, Normative Considerations, and Measurement Methods". In CHI Conference on Human Factors in Computing Systems (CHI '21). DOI: https://doi.org/10.1145/3411764.3445610

Mishra et al. (2020). "Don't count me out: On the relevance of IP addresses in the tracking ecosystem." The Web Conference 2020. DOI: https://dx.doi.org/10.1145/3366423.3380161

Munir et al. (2024). "Google's Chrome Antitrust Paradox." In Vanderbilt Journal of Entertainment & Technology Law, Vol. 27. https://web.cs.ucdavis.edu/~zubair/files/jetlaw-chrome-antitrust-paradox.pdf

Munir et al. (2023). "CookieGraph: Understanding and Detecting First-Party Tracking Cookies." In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23), DOI: https://doi.org/10.1145/3576915.3616586

Narayanan et al. (2020). "Dark Patterns: Past, Present, and Future: The evolution of tricky user interfaces." In March-April 2020 ACM Queue, Volume 18, Issue 2, pp 67-92. https://dl.acm.org/doi/pdf/10.1145/3400899.3400901

Olejnik et al. (2013). "Selling Off Privacy at Auction." https://inria.hal.science/hal-00915249/file/SellingOffPrivacyAtAuction.pdf

Reitinger et al. (2024). "What Does It Mean to Be Creepy? Responses to Visualizations of Personal Browsing Activity, Online Tracking, and Targeted Ads." In Proceedings on Privacy Enhancing Technologies (PoPETs), Volume 2024, Issue 3, pp 715-743. DOI: https://doi.org/10.56553/popets-2024-0101

Rescorla, E., Thomson, M. (2021). "Technical Comments on FLoC Privacy." https://mozilla.github.io/ppa-docs/floc_report.pdf

Sanchez-Rola, et al. (2021). "Journey to the Center of the Cookie Ecosystem: Unraveling Actors' Roles and Relationships." In 2021 IEEE Symposium on Security and Privacy (SP), pp 1990-2004. DOI: https://doi.org/10.1109/SP40001.2021.9796062

Servan-Schreiber et al (2021). "AdVeil: A Private Targeted-Advertising Ecosystem." In *IACR Cryptol. ePrint Arch., 2021*, 1032. https://eprint.iacr.org/2021/1032.pdf

Srinivasan, D. (2019). "Why Google Dominates Advertising Markets." In 24 STAN. TECH. L. REV. 55 (2020). https://ssrn.com/abstract=3500919

Su et al. (2017). "De-anonymizing Web Browsing Data with Social Networks." In Proceedings of the 26th International Conference on World Wide Web (WWW '17). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, pp 1261–1269. https://doi.org/10.1145/3038912.3052714

Tahaei, M., Vaniea, K. (2021). "'Developers Are Responsible': What Ad Networks Tell Developers About Privacy." In Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems (CHI EA '21), Article No.: 253, pp 1–11. DOI: https://doi.org/10.1145/3411763.3451805

Thomson, M. (2023). "A Privacy Analysis of Google's Topics Proposal." https://mozilla.github.io/ppa-docs/topics.pdf

Toubiana et al. (2010). "Adnostic: Privacy Preserving Targeted Advertising." In Proceedings Network and Distributed System Symposium. https://ssrn.com/abstract=2567076

Ur et al. (2012). "Smart, useful, scary, creepy: perceptions of online behavioral advertising." In Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12), Article 4, pp 1–15. DOI: https://doi.org/10.1145/2335356.2335362

Vekaria et al. (2022). "The Inventory is Dark and Full of Misinformation: Understanding the Abuse of Ad Inventory Pooling in the Ad-Tech Supply Chain." arXiv DOI: https://doi.org/10.48550/arXiv.2210.06654

Weinshel et al. (2019). "Oh, the Places You've Been! User Reactions to Longitudinal Transparency About Third-Party Web Tracking and Inferencing." In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), pp 149-166. DOI: https://doi.org/10.1145/3319535.3363200

G. Public Sources

Adalytics, "Is Google sharing data from Americans and Europeans with sanctioned Russian adtech companies?" https://adalytics.io/blog/sanctioned-ad-tech-user-data. Accessed August 19, 2024.

Angwin, J., "Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking," https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking. Accessed on August 8, 2024.

Auxier et al., "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/. Accessed on August 8, 2024.

Auxier, B., Anderson, M., "Social Media Use in 2021," https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/. Accessed August 19, 2024.

Cassidy et al., Letter to Sundar Pichai, Chief Executive Officer of Google LLC, (April 1, 2021) https://www.wyden.senate.gov/imo/media/doc/040121%20Wyden%20led%20Bidstream%20Letter%20to%20Google.pdf. Accessed August 28, 2024.

Commission Nationale de l'Informatique et des Libertés (CNIL – French Data Protection Authority), "Deliberation of the restricted committee No. SAN-2021-023 of 31 of December 2021 concerning GOOGLE LLC and GOOGLE IRELAND LIMITED," (December 31, 2021) https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-023_of_31_december_2021_concerning_google_llc_and_google_ireland_limited.pdf. Accessed August 16, 2024.

Congress.gov, "S.1974 - Protecting Americans' Data From Foreign Surveillance Act of 2023," https://www.congress.gov/bill/118th-congress/senate-bill/1974. Accessed August 27, 2024.

Cox, J., "Congress Says Foreign Intel Services Could Abuse Ad Networks for Spying," https://www.vice.com/en/article/88aw73/congress-foreign-intelligence-agencies-bidstream-real-time-bidding. Accessed August 19, 2024.

Cox, J., "The Hundreds of Little-Known Firms Getting Data on Americans," https://www.vice.com/en/article/hundreds-companies-bidstream-data-location-browsing/. Accessed August 27, 2024.

Deceptive Patterns, "Deliberation of the Restricted Committee concerning Google LLC and Google Ireland Limited," https://www.deceptive.design/cases/deliberation-of-the-restricted-committee-concerning-google-llc-and-google-ireland-limited. Accessed on August 8, 2024.

Deceptive Patterns, "Hall of shame: Hundreds of examples of deceptive patterns used by companies around the world," https://www.deceptive.design/hall-of-shame?brand=Google. Accessed August 19, 2024.

Deceptive Patterns, "Nagging," https://www.deceptive.design/types/nagging. Accessed August 19, 2024.

Deceptive Patterns, "What are deceptive patterns?" https://www.deceptive.design/. Accessed August 19, 2024.

Drummond, D., "An examination of the Google-DoubleClick merger and the online advertising industry: what are the risks for competition and privacy? Hearing before the subcommittee on antitrust,

competition policy and consumer rights of the Committee on the Judiciary United States Senate One Hundred Tenth Congress First session," (September 27, 2007) https://www.govinfo.gov/content/pkg/CHRG-110shrg39015/html/CHRG-110shrg39015.htm. Accessed on August 23, 2024.

DuckDuckGo, "tracker-radar/entities/Facebook, Inc..json," https://github.com/duckduckgo/tracker-radar/blob/main/entities/Facebook%2C%20Inc..json. Accessed August 29, 2024.

DuckDuckGo, "tracker-radar/entities/Microsoft Corporation.json," https://github.com/duckduckgo/tracker-radar/blob/main/entities/Microsoft%20Corporation.json. Accessed August 29, 2024.

DuckDuckGo, "tracker-radar/entities/Amazon Technologies, Inc..json," https://github.com/duckduckgo/tracker-radar/blob/main/entities/Amazon%20Technologies%2C%20Inc..json. Accessed August 29, 2024.

DuckDuckGo, "tracker-radar/entities/Google LLC.json," https://github.com/duckduckgo/tracker-radar/blob/main/entities/Google%20LLC.json. Accessed August 19, 2024.

European Data Protection Board, "The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC," https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en. Accessed August 16, 2024.

Federal Trade Commission, "Bringing Dark Patterns to Light," (September 2022) https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf. Accessed September 6, 2024.

Federal Trade Commission, "FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers: Tactics Include Disguised Ads, Difficult-to-Cancel Subscriptions, Buried Terms, and Tricks to Obtain Data," (September 15, 2022) https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers. Accessed September 6, 2024.

Federal Trade Commission, "In the matter of Google Inc., Corporation – Decision and order," (October 13, 2011) https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf. Accessed August 20, 2024.

Federal Trade Commission, "Statement of Federal Trade Commission concerning Google/DoubleClick FTC File No. 071-0170," (December 20, 2007) https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf. Accessed August 20, 2024.

Fung, B., "Gmail will no longer snoop on your emails for advertising purposes," https://www.washingtonpost.com/news/the-switch/wp/2017/06/26/gmail-will-no-longer-snoop-on-your-emails-for-advertising-purposes/. Accessed September 6, 2024.

Ghostery, "GHOSTERY WHOTRACKS.ME: Uncover who is tracking you online with WhoTracks.Me, featuring statistical reports derived from the web's largest open-source database of trackers," https://whotracks.me/. Accessed August 19, 2024.

Ghostery, "ORGANIZATION TRACKING REACH The chart illustrates the online tracking landscape across various organizations, depicting the extent of their reach," https://www.ghostery.com/whotracksme/tracking-reach. Accessed September 6, 2024.

Goldsmith, J., "France Slaps Google With €50M Fine For Privacy Violation Under GDPR," https://www.forbes.com/sites/jillgoldsmith/2019/01/21/france-slaps-google-with-e50m-fine-for-privacy-violation-under-gdpr/. Accessed August 16, 2024.

Google Chrome Help, "Manage your linked Google services," https://support.google.com/chrome/answer/14202892?hl=en&co=GENIE.Platform%3DAndroid. Accessed August 29, 2024.

Google, "2024 Google Ad Manager release archive: January 29 New joinable Bids Data Transfer file," https://support.google.com/admanager/answer/14438060#zippy=%2Cjanuary-new-joinable-bids-data-transfer-file. Accessed August 19, 2024.

Google, "Ads that respect your privacy," https://safety.google/privacy/ads-and-data/. Accessed August 19, 2024.

Google, "Authorized Buyers Real-time Bidding Proto," https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide#bidrequest-object. Accessed August 19, 2024.

Google, "Bids (joinable) data in Data Transfer," https://support.google.com/admanager/answer/13947328. Accessed August 19, 2024.

Google, "Cookie Matching," https://developers.google.com/authorized-buyers/rtb/cookie-guide. Accessed August 19, 2024.

Google, "European regulations overview and guidance Ad technology providers," https://support.google.com/admanager/answer/9012903. Accessed August 19, 2024.

Google, "OpenRTB Integration," https://developers.google.com/authorized-buyers/rtb/openrtb-guide. Accessed August 19, 2024.

Google, "Process the Request," https://developers.google.com/authorized-buyers/rtb/request-guide. Accessed August 19, 2024.

Google, "Real-time Bidding," https://developers.google.com/authorized-buyers/rtb/start. Accessed August 19, 2024.

Google, "Sign in and sync in Chrome," https://support.google.com/chrome/answer/185277?hl=en&co=GENIE.Platform%3DDesktop. Accessed September 6, 2024.

Greene, D., "As G Suite gains traction in the enterprise, G Suite's Gmail and consumer Gmail to more closely align," https://blog.google/products/gmail/g-suite-gains-traction-in-the-enterprise-g-suites-gmail-and-consumer-gmail-to-more-closely-align/. Accessed September 6, 2024.

Heine, F., "Google changes user data practices to end German antitrust probe," https://www.reuters.com/technology/german-cartel-office-google-users-have-better-control-over-their-data-2023-10-05/. Accessed August 16, 2024.

Jones Harbour, P., "In the matter of Google/DoubleClick F.T.C. File No. 071-0170 Dissenting statement of Commissioner Pamela Jones Harbour," (December 20, 2007) https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf. Accessed August 20, 2024.

Martin, N., "How Much Does Google Really Know About You? A Lot," https://www.forbes.com/sites/nicolemartin1/2019/03/11/how-much-does-google-really-know-about-you-a-lot/. Accessed August 29, 2024.

Oracle Data Cloud, "2019 Data Directory," https://web.archive.org/web/20210420081301/https://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf. Accessed August 19, 2024.

Perry, V., Hoffman, D., "George Talks Business- Donna Hoffman," https://www.youtube.com/watch?v=VVYPfmlUwmg. Accessed on August 8, 2024.

Ron Wyden United States Senator for Oregon, "Wyden Releases Draft Legislation to Protect Americans' Personal Data From Hostile Foreign Governments," https://www.wyden.senate.gov/news/press-releases/wyden-releases-draft-legislation-to-protect-americans-personal-data-from-hostile-foreign-governments. Accessed August 27, 2024.

Ron Wyden United States Senator for Oregon, "Wyden, Bipartisan Senators, Question Online Ad Exchanges on Sharing of Americans' Data with Foreign Companies," (April 02, 2021) https://www.wyden.senate.gov/news/press-releases/wyden-bipartisan-senators-question-online-ad-exchanges-on-sharing-of-americans-data-with-foreign-companies. Accessed August 28, 2024.

StatCounter, "Search Engine Market Share United States of America," https://gs.statcounter.com/search-engine-market-share/all/united-states-of-america. Accessed September 6, 2024.

Statista, "Market share of leading internet browsers in the United States and worldwide as of August 2024," https://www.statista.com/statistics/276738/worldwide-and-us-market-share-of-leading-internet-browsers. Accessed September 5, 2024.

Statista, "Most popular mapping apps in the United States as of April 2018, by reach," https://www.statista.com/statistics/865419/most-popular-us-mapping-apps-ranked-by-reach/. Accessed August 19, 2024.

Stigler Committee on Digital Platforms, "Final Report," (September 2019) https://research.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-

report---stigler-center.pdf?la=en&hash=2D23583FF8BCC560B7FEF7A81E1F95C1DDC5225E. Accessed August 28, 2024.

Sussman et al., "FTC AMICUS CURIAE BRIEF CASE NOS. 3:21-md-02981-JD; 3:20-cv-05671-JD," (August 12, 2024) https://www.ftc.gov/system/files/ftc_gov/pdf/ftc_amicus_brief_epic_v_google_play.pdf. Accessed August 28, 2024.

The Bundeskartellamt, "Decision pursuant to Section 19a(2) sentence 4 in conjunction with Section 32b(1) GWB - Public version," (June 10, 2023) https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2023/B7-70-21.pdf. Accessed August 16, 2024.

The Norwegian Consumer Council, "Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy," (June 27, 2018) https://storage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf. Accessed on August 19, 2024.

Vincent J., "France fines Google and Facebook for pushing tracking cookies on users with dark patterns / One button to accept all — but not to reject all," https://www.theverge.com/2022/1/7/22871719/france-fines-google-facebook-cookies-tracking-dark-patterns-eprivacy. Accessed on August 8, 2024.

VIII. APPENDIX C: CURRICULUM VITAE OF DR. ZUBAIR SHAFIQ

[DOCUMENT BEGINS ON THE FOLLOWING PAGE]

3043 Kemper Hall
Davis, CA, 95616 USA
zubair@ucdavis.edu
www.cs.ucdavis.edu/~zubair

Zubair Shafiq

Research Interests

Web Privacy, Internet Measurement, Internet Security, Computer Networks

Professional Experience

2020– **Associate Professor**
Department of Computer Science, University of California-Davis

2014–2020 **Assistant Professor**
Department of Computer Science, University of Iowa

2009–2014 **Research Assistant**
Department of Computer Science and Engineering, Michigan State University

2013 **Research Intern**
IBM T. J. Watson Research Center

2012 **Research Intern**
Telefonica Research

2011 **Research Intern**
AT&T Labs – Research

2007-2009 **Research Engineer**
Next Generation Intelligent Networks Research Center, Pakistan

Education

2009–2014 **Ph.D. Computer Science**
Department of Computer Science and Engineering, Michigan State University

2004–2008 **B.E. Electrical Engineering**
National University of Sciences & Technology (NUST), Pakistan

Honors and Awards

2024 **Caspar Bowden Award**, Runner-up for Outstanding Research in Privacy Enhancing Technologies
2023 **Best Paper Award**, ACM Internet Measurement Conference
2023 **Chancellor's Fellow**, University of California Davis
2020 **Research Highlights**, Communications of the ACM
2020 **Dean's Scholar Award**, University of Iowa
2018 **NSF Faculty Early Career Development (CAREER) Award**
2018 **Andreas Pfitzmann Award**, Best Student Paper at Privacy Enhancing Technologies Symposium
2017 **Best Paper Award**, ACM Internet Measurement Conference
2015 **NSF CISE Research Initiation Initiative (CRII) Award**
2013 **Fitch-Beach Outstanding Graduate Research Award**, Michigan State University
2012 **Best Paper Award**, IEEE International Conference on Network Protocols

2007, 2008 **Dean's Plaque of Excellence**, National University of Sciences & Technology, Pakistan

Publications

ICWSM **Towards Characterizing and Detecting Incentivized Reviews on eCommerce Platforms**
Rajvardhan Oak, Zubair Shafiq
AAAI International Conference on Web and Social Media, 2025

IMC **Watching TV with the Second-Party: A First Look at Automatic Content Recognition Tracking in Smart TVs**
Abdul Haddi Amjad, Shaoor Munir, Zubair Shafiq, Muhammad Ali Gulzar
ACM Internet Measurement Conference, 2024

CCS **Blocking Tracking JavaScript at the Function Granularity**
Gianluca Anselmi, Yash Vekaria, Alexander D'Souza, Patricia Callejo, Anna Maria Mandalari, Zubair Shafiq
ACM Conference on Computer and Communications Security, 2024

USENIX Security **PURL: Safe and Effective Sanitization of Link Decoration**
Shaoor Munir, Patrick Lee, Umar Iqbal, Zubair Shafiq, Sandra Siby
USENIX Security Symposium, 2024

JETLaw **Google's Chrome Antitrust Paradox**
Shaoor Munir, Konrad Kollnig, Anastasia Shuba, Zubair Shafiq
Vanderbilt Journal of Entertainment and Technology Law, 2024

IMWUT/ UbiComp **Aragorn: A Privacy-Enhancing System for Mobile Cameras**
Hari Venugopalan, Zainul Abi Din, Trevor Carpenter, Jason Lowe-Power, Sam King, Zubair Shafiq
ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2024

CHI **Understanding Underground Incentivized Review Services**
Rajvardhan Oak, Zubair Shafiq
ACM Conference on Human Factors in Computing Systems, 2024

S&P **The Inventory is Dark and Full of Misinformation: Understanding the Abuse of Ad Inventory Pooling in the Ad-Tech Supply Chain**
Yash Vekaria, Rishab Nithyanand, Zubair Shafiq
IEEE Symposium on Security & Privacy, 2024

JOLT **A Scientific Approach to Tech Accountability**
Woodrow Hartzog, Scott Jordan, David Choffnes, Athina Markopoulou, Zubair Shafiq
Beyond the FTC: The Future of Privacy Enforcement, Harvard Journal of Law & Technology, 2023

PNAS **Auditing YouTube's Recommendation System for Ideologically Congenial, Extreme, and Problematic Recommendations**
Muhammad Haroon, Magdalena Wojcieszak, Anshuman Chhabra, Xin Liu, Prasant Mohapatra, Zubair Shafiq
Proceedings of the National Academy of Sciences (PNAS), 2023

IMC **Tracking, Profiling, and Ad Targeting in the Alexa Echo Smart Speaker Ecosystem**
Umar Iqbal, Pouneh Nikkhah Bahrami, Rahmadi Trimananda, Hao Cui, Alexander Gamero-Garrido, Daniel Dubois, David Choffnes, Athina Markopoulou, Franziska Roesner, Zubair Shafiq
ACM Internet Measurement Conference, 2023
Best Paper Award

PETS **A Utility-Preserving Obfuscation Approach for YouTube Recommendations**
Jiang Zhang, Hadi Askari, Konstantinos Psounis, Zubair Shafiq
Privacy Enhancing Technologies Symposium, 2023

PETS **Blocking JavaScript without Breaking the Web**
Abdul Haddi Amjad, Zubair Shafiq, Muhammad Ali Gulzar
Privacy Enhancing Technologies Symposium, 2023

CCS **CookieGraph: Measuring and Countering First-Party Tracking Cookies**
Shaoor Munir, Sandra Siby, Umar Iqbal, Steven Englehardt, Zubair Shafiq, Carmela Troncoso
ACM Conference on Computer and Communications Security, 2023

S&P **Accuracy-Privacy Trade-off in Deep Ensemble: A Membership Inference Perspective**
Shahbaz Rezaei, Zubair Shafiq, Xin Liu
IEEE Symposium on Security & Privacy, 2023

USENIX Security **AutoFR: Automated Filter Rule Generation for Adblocking**
Hieu Le, Salma Elmalaki, Athina Markopoulou, Zubair Shafiq
USENIX Security Symposium, 2023

NDSS **Harpo: Learning to Subvert Online Behavioral Advertising**
Jiang Zhang, Konstantinos Psounis, Muhammad Haroon, Zubair Shafiq
Network and Distributed System Security Symposium, 2022

USENIX Security **WebGraph: Capturing Advertising and Tracking Information Flows for Robust Blocking**
Sandra Siby, Umar Iqbal, Steven Englehardt, Zubair Shafiq, Carmela Troncoso
USENIX Security Symposium, 2022

USENIX Security **Khaleesi: Breaker of Advertising and Tracking Request Chains**
Umar Iqbal, Charlie Wolfe, Charles Nguyen, Steven Englehardt, Zubair Shafiq
USENIX Security Symposium, 2022

PETS **FP-Radar: Longitudinal Measurement and Early Detection of Browser Fingerprinting**
Pouneh Nikkhah Bahrami, Umar Iqbal, Zubair Shafiq
Privacy Enhancing Technologies Symposium, 2022

ACL **Adversarial Authorship Attribution for Deobfuscation**
Wanyue Zhai, Jonathan Rusert, Zubair Shafiq, Padmini Srinivasan
Association for Computational Linguistics, 2022

ACL **On the Robustness of Offensive Language Classifiers**
Jonathan Rusert, Zubair Shafiq, Padmini Srinivasan
Association for Computational Linguistics, 2022

EuroS&P **DNN Model Architecture Fingerprinting Attack on CPU-GPU Edge Devices**
Kartik Patwari, Syed Mahbub Hafiz, Han Wang, Houman Homayoun, Zubair Shafiq, Chen-Nee Chuah
IEEE European Symposium on Security and Privacy, 2022

DATE **Stealthy Inference Attack on DNN via Cache-based Side-channel Attacks**
Han Wang, Syed Mahbub Hafiz, Kartik Patwari, Chen-Nee Chuah, Zubair Shafiq, Houman Homayoun
IEEE/ACM Design Automation and Test in Europe, 2022

IMC **TrackerSift: Untangling Mixed Tracking and Functional Web Resources**
Abdul Haddi Amjad, Danial Saleem, Fareed Zaffar, Muhammad Ali Gulzar, Zubair Shafiq
ACM Internet Measurement Conference, 2021

S&P **Fingerprinting the Fingerprinters: Learning to Detect Browser Fingerprinting Behaviors**
Umar Iqbal, Steven Englehardt, Zubair Shafiq
IEEE Symposium on Security & Privacy, 2021

NDSS **CV-Inspector: Towards Automating Detection of Adblock Circumvention**
Hieu Le, Athina Markopoulou, Zubair Shafiq
Network and Distributed System Security Symposium, 2021

EACL **Through the Looking Glass: Learning to Attribute Synthetic Text Generated by Language Models**
Shaoor Munirl, Brishna Batool, Zubair Shafiq, Padmini Srinivasan, Fareed Zaffar
European Chapter of the Association for Computational Linguistics, 2021

IMC **Understanding Incentivized Mobile App Installs on Google Play Store**
Shehroze Farooqi, Alvaro Feal, Tobias Lauinger, Damon McCoy, Zubair Shafiq, Narseo Vallina-Rodriguez
ACM Internet Measurement Conference, 2020

ACL **A Girl Has A Name: Detecting Authorship Obfuscation**
Asad Mahmood, Zubair Shafiq, Padmini Srinivasan
Annual Conference of the Association for Computational Linguistics, 2020

S&P **AdGraph: A Graph-Based Approach to Ad and Tracker Blocking**
Umar Iqbal, Peter Snyder, Shitong Zhu, Benjamin Livshits, Zhiyun Qian, Zubair Shafiq
IEEE Symposium on Security & Privacy, San Francisco, 2020

PETS **CanaryTrap: Detecting Data Misuse by Third-Party Apps on Online Social Networks**
Shehroze Farooqi, Maaz Musa, Zubair Shafiq, Fareed Zaffar
Privacy Enhancing Technologies Symposium, Montreal, 2020

PETS **Inferring Tracker-Advertiser Relationships in the Online Advertising Ecosystem**
John Cook, Rishab Nithyanand, Zubair Shafiq
Privacy Enhancing Technologies Symposium, Montreal, 2020

PETS **The TV is Smart and Full of Trackers: Measuring Smart TV Advertising and Tracking**
Janus Varmarken, Hieu Le, Anastasia Shuba, Zubair Shafiq, Athina Markopoulou
Privacy Enhancing Technologies Symposium, Montreal, 2020

IoTDI **Characterizing Smart Home IoT Traffic in the Wild**
M. Hammad Mazhar, Zubair Shafiq
ACM/IEEE Conference on Internet of Things Design and Implementation, Sydney, 2020

PAM **FlowTrace: A Framework for Active Bandwidth Measurements using In-band Packet Trains**
Adnan Ahmed, Ricky Mok, Zubair Shafiq
Passive and Active Measurement Conference, Eugene, 2020

PETS **A Girl Has No Name: Automated Authorship Obfuscation using X-Mutant**
Asad Mahmood, Faizan Ahmad, Zubair Shafiq, Padmini Srinivasan, Fareed Zaffar
Privacy Enhancing Technologies Symposium, Stockholm, 2019

PETS **No Place to Hide: Inadvertent Location Privacy Leaks on Twitter**
Jonathan Rusert, Osama Khalid, Dat Hong, Zubair Shafiq, Padmini Srinivasan
Privacy Enhancing Technologies Symposium, Stockholm, 2019

WWW **Measurement and Early Detection of Third-Party Application Abuse on Twitter**
Shehroze Farooqi, Zubair Shafiq
The Web Conference (WWW), San Francisco, 2019

WWW **ShadowBlock: A Lightweight and Stealthy Adblocking Browser**
Shitong Zhu, Umar Iqbal, Zhongjie Wang, Zhiyun Qian, Zubair Shafiq, Weiteng Chen
The Web Conference (WWW), San Francisco, 2019

WWW **Measuring Political Personalization of Google News Search**
Huyen Le, Raven Maragh, Brian Ekdale, Timothy Havens, Andrew High, Zubair Shafiq
The Web Conference (WWW), San Francisco, 2019

ASONAM **A Postmortem of Suspended Twitter Accounts in the 2016 U.S. Presidential Election**
Huyen Le, Bob Boynton, Zubair Shafiq, Padmini Srinivasan
IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), Vancouver, 2019

TDSC **Large Scale Characterization of Software Vulnerability Life Cycles**
Muhammad Shahzad, Zubair Shafiq, Alex X. Liu
IEEE Transactions on Dependable and Secure Computing, 2019

PETS **NoMoAds: Effective and Efficient Cross-App Mobile Ad-Blocking**
Anastasia Shuba, Athina Markopoulou, Zubair Shafiq
Privacy Enhancing Technologies Symposium, Barcelona, 2018
Andreas Pfitzmann Best Student Paper Award

NDSS **Measuring and Disrupting Anti-Adblockers Using Differential Execution Analysis**
Shitong Zhu, Xunchao Hu, Zhiyun Qian, Zubair Shafiq, Heng Yin
Network and Distributed System Security Symposium, San Diego, 2018

INFOCOM **Real-time Video Quality of Experience Monitoring for HTTPS and QUIC**
M. Hammad Mazhar, Zubair Shafiq
IEEE International Conference on Computer Communications, Honolulu, 2018

TON **Optimizing Internet Transit Routing for Content Delivery Networks**
Faraz Ahmed, Zubair Shafiq, Amir Khakpour, Alex Liu
IEEE/ACM Transactions on Networking, 2018

TBD **Optimizing Taxi Driver Profit Efficiency: A Spatial Network-based Markov Decision Process Approach**
Xun Zhou, Huigui Rong, Chang Yang, Qun Zhang, Amin Vahedian Khezerlou, Hui Zheng, Zubair Shafiq, Alex Liu
IEEE Transactions on Big Data, 2018

TOPS **Measuring, Characterizing, and Detecting Facebook Like Farms**
Muhammad Ikram, Lucky Onwuzurike, Shehroze Farooqi, Emiliano De Cristofaro, Arik Friedman, Guillaume Jourjon, Dali Kaafar, Zubair Shafiq
ACM Transactions on Privacy and Security, 2017

TIST **A Traffic Flow Approach to Early Detection of Gathering Events: Comprehensive Results**
Amin Khezerlou, Xun Zhou, Lufan Li, Zubair Shafiq, Alex X. Liu, Fan Zhang
ACM Transactions on Intelligent Systems and Technology, 2017

IMC **Measuring and Mitigating OAuth Access Token Abuse by Collusion Networks**
Shehroze Farooqi, Fareed Zaffar, Nektarios Leontiadis, Zubair Shafiq
ACM Internet Measurement Conference, London, 2017
Best Paper Award
CACM Research Highlights 2020

IMC **The Ad Wars: Retrospective Measurement and Analysis of Anti-Adblock Filter Lists**
Umar Iqbal, Zubair Shafiq, Zhiyun Qian
ACM Internet Measurement Conference, London, 2017

SIGMETRICS **Characterizing and Modeling Patching Practices of Industrial Control Systems**
Brandon Wang, Xiaoye Li, Leandro P. de Aguiar, Daniel S. Menasche, Zubair Shafiq
ACM International Conference on Measurement and Modeling of Computer Systems, Urbana-Champaign, 2017

PETS **Detecting Anti Ad-blockers in the Wild**
Muhammad Haris Mughees, Zhiyun Qian, Zubair Shafiq
Privacy Enhancing Technologies Symposium, Minneapolis, 2017

ICDM **Accurate Detection of Automatically Spun Content via Stylometric Analysis**
Usman Shahid, Shehroze Farooqi, Raza Ahmad, Zubair Shafiq, Padmini Srinivasan, Fareed Zaffar
IEEE International Conference on Data Mining, New Orleans, 2017

CHI **Revisiting The American Voter on Twitter**
Huyen Le, G.R. Boynton, Yelena Mejova, Zubair Shafiq, Padmini Srinivasan
ACM Conference on Human Factors in Computing Systems, Denver, 2017

ICDCS **Distributed Load Balancing in Key-Value Networked Caches**
Sikder Huq, Zubair Shafiq, Sukumar Ghosh, Amir Khakpour, Harkeerat Bedi
IEEE International Conference on Distributed Computing Systems, Atlanta, 2017

ICNP **Peering vs. Transit: Performance Comparison of Peering and Transit Interconnections**
Adnan Ahmed, Zubair Shafiq, Harkeerat Bedi, Amir Khakpour
IEEE International Conference on Network Protocols, Toronto, 2017

ICNP **Suffering from Buffering? Detecting QoE Impairments in Live Video Streams**
Adnan Ahmed, Zubair Shafiq, Harkeerat Bedi, Amir Khakpour
IEEE International Conference on Network Protocols, Toronto, 2017

ICNP **Multipath TCP Traffic Diversion Attacks and Countermeasures**
Ali Munir, Zhiyun Qian, Zubair Shafiq, Alex Liu, Franck Le
IEEE International Conference on Network Protocols, Toronto, 2017

ICWSM **Scalable News Slant Measurement Using Twitter**
Huyen Le, Zubair Shafiq, Padmini Srinivasan
AAAI International Conference on Web and Social Media, 2017

HT **Bumps and Bruises: Mining Presidential Campaign Announcements on Twitter**
Huyen Le, G.R. Boynton, Yelena Mejova, Zubair Shafiq, Padmini Srinivasan
ACM Conference on Hypertext and Social Media, Prague, 2017

Networking **Cascade Size Prediction in Online Social Networks**
Zubair Shafiq, Alex Liu
IFIP Networking, Prague, 2017
Best Paper Award Candidate (3 nominations out of 43 accepted papers)

Networking **A Graph Theoretic Approach to Fast and Accurate Malware Detection**
Zubair Shafiq, Alex Liu
IFIP Networking, Prague, 2017

eCrime **Characterizing Key Stakeholders in an Online Black-Hat Marketplace**
Shehroze Farooqi, Muhammad Ikram, Emiliano De Cristofaro, Arik Friedman, Guillaume Jourjon, Dali Kaafar, Zubair Shafiq, Fareed Zaffar
IEEE/APWG Symposium on Electronic Crime Research, Prague, 2017

ICNP **Optimizing Internet Transit Routing for Content Delivery Networks**
Faraz Ahmed, Zubair Shafiq, Amir Khakpour, Alex Liu
IEEE International Conference on Network Protocols, Singapore, 2016

DSN **Malware Slums: Measurement and Analysis of Malware on Traffic Exchanges**
Salman Yousaf, Umar Iqbal, Shehroze Farooqi, Raza Ahmad, Zubair Shafiq, Fareed Zaffar
IEEE/IFIP International Conference on Dependable Systems and Networks, France, 2016

SIGMETRICS **QoE Analysis of a Large-Scale Live Video Streaming Event**
Adnan Ahmed, Zubair Shafiq, Amir R. Khakpour
ACM International Conference on Measurement and Modeling of Computer Systems, France, 2016

ICDCS **The Internet is For Porn: Measurement and Analysis of Online Adult Traffic**
Faraz Ahmed, Zubair Shafiq, Alex X. Liu
IEEE International Conference on Distributed Computing Systems, Japan, 2016

INFOCOM **Characterizing Caching Workload of a Large Commercial Content Delivery Network**
Zubair Shafiq, Amir R. Khakpour, Alex X. Liu
IEEE International Conference on Computer Communications, San Francisco, 2016

SIGSPATIAL **A Traffic Flow Approach to Early Detection of Gathering Events**
Xun Zhou, Amin Vahedian Khezerlou, Alex Liu, Zubair Shafiq, Fan Zhang
ACM International Conference on Advances in Geographic Information Systems, San Francisco, 2016

CIKM **The Rich and the Poor: A Markov Decision Process Approach to Optimizing Taxi Driver Revenue Efficiency**
Huigui Rong, Xun Zhou, Chang Yang, Zubair Shafiq, Alex Liu
ACM International Conference on Information and Knowledge Management, Indianapolis, 2016

TON **Characterizing and Optimizing Cellular Network Performance during Crowded Events**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Shobha Venkataraman, Jia Wang
IEEE/ACM Transactions on Networking, 2016

SMP **What Campaigns Become as Social Media Become the Infrastructure of Political Communication**
G.R. Boynton, Huyen Le, Yelena Mejova, Zubair Shafiq, Padmini Srinivasan
Social Media and Politics, 2016

TMC **Geospatial and Temporal Dynamics of Application Usage in Cellular Data Networks**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang
IEEE Transactions on Mobile Computing, 2015

NSF/FCC QoE **Tracking Mobile Video QoE in the Encrypted Internet**
Zubair Shafiq
NSF/FCC Workshop on Tracking Quality of Experience in the Internet, Princeton, 2015

NSF/FCC QoE **Bidirectional Crosslayer QoE Optimization**
Srikanth Sundaresan, Zubair Shafiq
NSF/FCC Workshop on Tracking Quality of Experience in the Internet, Princeton, 2015

IMC **Paying for Likes? Understanding Facebook Like Fraud Using Honeypots**
Emiliano De Cristofaro, Arik Friedmam, Guillaume Jourjon, Dali Kaafar, Zubair Shafiq
ACM Internet Measurement Conference, 2014

SIGMETRICS **Understanding the Impact of Network Dynamics on Mobile Video User Engagement**
Zubair Shafiq, Jeffrey Erman, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang
ACM International Conference on Measurement and Modeling of Computer Systems, 2014

SIGMETRICS **Revisiting Caching in Content Delivery Networks**
Zubair Shafiq, Alex X. Liu, Amir Khakpour
ACM International Conference on Measurement and Modeling of Computer Systems, 2014

SIGMETRICS **A First Look at Cellular Network Performance during Crowded Events**
Zubair Shafiq, Alex X. Liu, Amir Khakpour
ACM International Conference on Measurement and Modeling of Computer Systems, 2013

ICNP **Who are You Talking to? Breaching Privacy in Encrypted IM Networks**
Muhammad U. Ilyas, Zubair Shafiq, Alex X. Liu, Hayder Radha
IEEE International Conference on Network Protocols, 2013

CSCW **Is News Sharing on Twitter Ideologically Biased?**
Jonathan Morgan, Cliff Lampe, Zubair Shafiq
ACM Conference on Computer Supported Cooperative Work and Social Computing, 2013

ACM HotNets **Cross-Path Inference Attacks on Multipath TCP**
Zubair Shafiq, Franck Le, Mudhakar Srivatsa, Alex X. Liu
ACM Workshop on Hot Topics in Networks, 2013

TON **Large Scale Measurement and Characterization of Cellular Machine-to-Machine Traffic**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang
IEEE/ACM Transactions on Networking, 2013

JSAC **Identifying Leaders and Followers in Online Social Networks**
Zubair Shafiq, Muhammad U. Ilyas, Alex X. Liu, Hayder Radha
IEEE Journal on Selected Areas in Communications, 2013

JSAC **A Distributed Algorithm for Identifying Information Hubs in Social Networks**
Muhammad U. Ilyas, Zubair Shafiq, Alex X. Liu, Hayder Radha
IEEE Journal on Selected Areas in Communications, 2013

JNSM **TCAMChecker: A Software Approach to the Error Detection and Correction of TCAM-based Networking Systems**
Zubair Shafiq, Chad Meiners, Alex Liu, Ke Shen, Zheng Qin
Springer Journal of Network and Systems Management, 2012

ICNP **A Semantics Aware Approach to Automated Reverse Engineering Unknown Protocols**
Yipeng Wang, Xiaochun Yun, Zubair Shafiq, Alex X. Liu, Zhibin Zhang, Liyan Wang, Danfeng (Daphne) Yao, Yongzheng Zhang, Li Guo
IEEE International Conference on Network Protocols, 2012
Best Paper Award

SIGMETRICS **A First Look at Cellular Machine-to-Machine Traffic – Large Scale Measurement and Characterization**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang
ACM International Conference on Measurement and Modeling of Computer Systems, London, 2012

ICSE **A Large Scale Exploratory Analysis of Software Vulnerability Life Cycles**
Muhammad Shahzad, Zubair Shafiq, Alex X. Liu
International Conference on Software Engineering, Switzerland, 2012

INFOCOM **Characterizing Geospatial Dynamics of Application Usage in a 3G Cellular Data Network**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang
IEEE Conference on Computer Communications, Orlando, 2012

SIGMETRICS **Characterizing and Modeling Internet Traffic Dynamics of Cellular Devices**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jia Wang
ACM International Conference on Measurement and Modeling of Computer Systems, San Jose, 2011

Networking **A Random Walk Approach to Modeling the Dynamics of the Blogosphere**
Zubair Shafiq, Alex X. Liu
IFIP Networking, Spain, 2011

INFOCOM **A Distributed and Privacy-Preserving Algorithm for Identifying Information Hubs in Social Networks**
Muhammad U. Ilyas, Zubair Shafiq, Alex X. Liu, Hayder Radha
IEEE Conference on Computer Communications, Spain, 2011

RAID **PE-Miner: Mining Structural Information to Detect Malicious Executables in Realtime**
Zubair Shafiq, Syeda Momina Tabish, Fauzan Mirza, Muddassar Farooq
International Symposium On Recent Advances In Intrusion Detection, France, 2009

GECCO **Evolvable Malware**
Sadia Noreen, Shafaq Murtaza, Zubair Shafiq, Muddassar Farooq
ACM Genetic and Evolutionary Computation Conference, Canada, 2009

CCS AISec **Using Spatio-Temporal Information in API Calls with Machine Learning Algorithms for Malware Detection and Analysis**
Faraz Ahmed, Haider Hameed, Zubair Shafiq, Muddassar Farooq
Workshop on Security and Artificial Intelligence, ACM Conference on Computer & Communications Security, Chicago, 2009

KDD CSI **Malware Detection using Statistical Analysis of Byte-Level File Content**
Syeda Momina Tabish, Zubair Shafiq, Muddassar Farooq
Workshop on CyberSecurity and Intelligence Informatics (CSI), ACM Conference on Knowledge Discovery and Data Mining, France, 2009

VB **PE-Probe: leveraging packer detection and structural information to detect malicious portable executables**
Zubair Shafiq, Syeda Momina Tabish, Muddassar Farooq
Virus Bulletin, Switzerland, 2009

Elsevier **Fuzzy Case Based Reasoning for Facial Expression Recognition**
Aasia Khanum, Muid Mufti, M. Y. Javed, Zubair Shafiq
Elsevier Fuzzy Sets and Systems, 2009

EvoComNet **A Comparative Study of Fuzzy Inference Systems, Neural Networks and Adaptive Neuro Fuzzy Inference Systems for Portscan Detection**
Zubair Shafiq, Muddassar Farooq, Syed Ali Khayam
Applications of Evolutionary Computing, EvoComNet, Italy, 2008

DIMVA **Embedded Malware Detection using Markov n-grams**
Zubair Shafiq, Syed Ali Khayam, Muddassar Farooq
International Conference on Detection of Intrusions, Malware and Vulnerability Assessment, France, 2008

GECCO **Improving Accuracy of Immune Inspired Malware Detectors using Intelligent Features**
Zubair Shafiq, Syed Ali Khayam, Muddassar Farooq
ACM Genetic and Evolutionary Computation Conference, Atlanta, 2008

Funding

External Competitive Research Grants

NSF-SaTC-EAGER **News and Public Affairs Information**
National Science Foundation
PI, Duration: 2024-2026, Total: $300,000, Personnel: Magdalena Wojcieszak (PI), Zubair Shafiq (Co-PI)

UC **Auditing Compliance of Data Privacy Laws in California**
UC Partnerships in Computational Transformation
PI, Duration: 2022-2023, Total: $160,000, Share: $80,000
Personnel: Zubair Shafiq (PI: UC Davis); Athina Markopoulou (PI: UC Irvine); Gene Tsudik (Co-PI: UC Irvine)

NSF-SaTC **Defending against Emerging Stateless Web Tracking**
National Science Foundation
PI, Duration: 2022-2026, Total: $1,200,000, Share: $400,000
Personnel: Zubair Shafiq (PI: UC Davis); Alexandros Kapravelos (PI: NC State); Anupam Das (Co-PI: NC State)

CITRIS and the Banatao Institute **Auditing the compliance of California consumer privacy regulations at scale**
Center for Information Technology Research in the Interest of Society (CITRIS)
Co-PI, Duration: 2021-2022, Total: $60,000, Share: $20,000
Personnel: Serge Egelman (Co-PI: UC Berkeley); Zubair Shafiq (Co-PI: UC Davis)

NSF-SaTC-Frontier **Protecting Personal Data Flow on the Internet**
National Science Foundation
PI, Duration: 2020-2025, Total: $10,000,000, Share: $1,100,000
Personnel: Zubair Shafiq (PI: UC Davis); Athina Markopoulou (PI: UC Irvine); Konstantinos Psounis (PI: USC); David Choffnes (PI: Northeastern)

NSF-CAREER **Quality of Experience and Network Management in the Encrypted Internet**
National Science Foundation
PI, Duration: 2018-2023, Total: $500,000, Share: $500,000
Personnel: Zubair Shafiq (PI: UC Davis)

NSF-SaTC **A Multi-Layer Learning Approach to Mobile Traffic Filtering**
National Science Foundation
PI, Duration: 2018-2021, Total: $500,000, Share: $250,000
Personnel: Zubair Shafiq (PI: UC Davis); Athina Markopoulou (PI: UC Irvine)

NSF-SaTC **The Web Ad Technology Arms Race: Measurement, Analysis, and Countermeasures**
National Science Foundation
PI, Duration: 2017-2020, Total: $500,000 + $16,000 (REU Supplement 2019) + $16,000 (REU Supplement 2021), Share: $282,000
Personnel: Zubair Shafiq (PI: UC Davis); Zhiyun Qian (PI: UC Riverside)

NSF-NeTS **Towards Scalable and Energy Efficient Cellular IoT Communication**
National Science Foundation
PI, Duration: 2016-2019, Total: $500,000, Share: $166,000
Personnel: Zubair Shafiq (PI: Iowa); K.K. Ramakrishnan (PI: UC Riverside); Koushik Kar (PI: RPI)

NSF-SaTC **Multipath TCP Side Channel Vulnerabilities and Defenses**
National Science Foundation
PI, Duration: 2015-2018, Total: $500,000, Share: $167,000
Personnel: Zubair Shafiq (PI: Iowa); Zhiyun Qian (PI: UC Riverside); Alex Liu (PI: Michigan State University)

NSF-NeTS **Towards Measurement and Optimization of Internet Video Quality of Experience**
National Science Foundation
PI, Duration: 2015-2018, Total: $175,000 + $16,000 (REU Supplement 2016), Share: $191,000
Personnel: Zubair Shafiq (PI: Iowa)

DTL **Detection and Circumvention of Ad-Block Detectors**
Data Transparency Lab
PI, Duration: 2016-2017, Total: $56,000, Share: $28,000
Personnel: Zubair Shafiq (PI: Iowa); Zhiyun Qian (PI: UC Riverside)

Internal Competitive Research Grants

Academic Senate **Socio-Computational Interventions to Mitigate Misinformation in Recommendations**
Noyce Foundation
PI, Duration: 2022-2023, Total: $25,000
Personnel: Magdalena Wojcieszak (PI), Zubair Shafiq (Co-PI)

Noyce **Measuring and Mitigating Biases in Social Recommendation Algorithms**
Noyce Foundation
PI, Duration: 2022-2023, Total: $236,000
Personnel: Zubair Shafiq (PI), Magdalena Wojcieszak (Co-PI)

Noyce **Cross-Layer Approach to Enhance Security/Privacy of AI-enabled IoT Eco-Systems**
Noyce Foundation
Co-PI, Duration: 2022-2023, Total: $225,000
Personnel: Chen-Nee Chuah (PI), Zubair Shafiq (Co-PI), Houman Homayoun (Co-PI)

Noyce **Measuring and Mitigating Biases in Social Recommendation Algorithms**
Noyce Foundation
PI, Duration: 2021-2022, Total: $235,690
Personnel: Zubair Shafiq (PI), Xin Liu (Co-PI), Magdalena Wojcieszak (Co-PI)

Noyce **Cross-Layer Approach to Enhance Security/Privacy of AI-enabled IoT Eco-Systems**
Noyce Foundation
Co-PI, Duration: 2021-2022, Total: $225,000
Personnel: Chen-Nee Chuah (PI), Zubair Shafiq (Co-PI), Houman Homayoun (Co-PI)

UIRF **Social Media Powered Real-Time Digital News Recommendation**
University of Iowa Research Foundation
PI, Duration: 2015-2016, Total: $75,000
Personnel: Zubair Shafiq (PI)

Obermann **Heterogeneous Network Data Analytics to Improve Urban Sustainability**
Obermann Center Interdisciplinary Research Grant
PI, Duration: 2015-2016, Total: $12,000
Personnel: Xun Zhou (PI); Zubair Shafiq (Co-PI)

Industry Grants and Unrestricted Gifts

Siemens PI, Duration: 2021, Total: $60,000, Share: $60,000
Personnel: Zubair Shafiq (PI: UC Davis)

Siemens	PI, Duration: 2019, Total: $30,000, Share: $30,000 Personnel: Zubair Shafiq (PI: Iowa)
Siemens	PI, Duration: 2018, Total: $60,000, Share: $60,000 Personnel: Zubair Shafiq (PI: Iowa)
Verizon	PI, Duration: 2018, Total: $20,000, Share: $20,000 Personnel: Zubair Shafiq (PI: Iowa)
Minim	PI, Duration: 2018, Total: $66,164, Share: $66,164 Personnel: Zubair Shafiq (PI: Iowa)
Siemens	PI, Duration: 2017, Total: $30,000, Share: $30,000 Personnel: Zubair Shafiq (PI: Iowa)
Nokia	PI, Duration: 2017, Total: $53,200, Share: $53,200 Personnel: Zubair Shafiq (PI: Iowa)
Futurewei	PI, Duration: 2017, Total: $100,384, Share: $100,384 Personnel: Zubair Shafiq (PI: Iowa)
Facebook	PI, Duration: 2016, Total: $8,400, Share: $8,400 Personnel: Zubair Shafiq (PI: Iowa)

Teaching

ECS 289M	**Topics in Privacy** Spring 2024, University of California at Davis
ECS 188	**Ethics in an Age of Technology** Winter 2024, University of California at Davis
ECS 152A	**Computer Networks** Fall 2023, University of California at Davis
FYS	**Big Data, Big Brother** Winter 2023, University of California at Davis
ECS 289M	**Network Security & Privacy** Winter 2023, University of California at Davis
ECS 152A	**Computer Networks** Fall 2022, University of California at Davis
ECS 152A	**Computer Networks** Spring 2022, University of California at Davis
ECS 153	**Computer Security** Winter 2022, University of California at Davis
ECS 289M	**Data-Driven Security** Spring 2021, University of California at Davis
ECS 152B	**Computer Networks** Winter 2021, University of California at Davis
CS 2620	**Networking & Security for Informatics** Spring 2020, The University of Iowa
CS 4980	**Online Advertising & Tracking** Fall 2019, The University of Iowa

CS 2620 **Networking & Security for Informatics**
Spring 2019, The University of Iowa

CS 4980 **Internet Measurement**
Fall 2018, The University of Iowa

CS 2620 **Networking & Security for Informatics**
Spring 2018, The University of Iowa

CS 2620 **Networking & Security for Informatics**
Spring 2017, The University of Iowa

CS 4980 **Network Security and Privacy**
Fall 2016, The University of Iowa

CS 2620 **Networking & Security for Informatics**
Spring 2016, The University of Iowa

CS 4980 **Advanced Computer Networks**
Fall 2015, The University of Iowa

CS 2620 **Networking & Security for Informatics**
Spring 2015, The University of Iowa

CS 4980 **Internet Measurement**
Fall 2014, The University of Iowa

Students

Doctorate

2022-current Rajvardhan Oak
2021-current Pouneh Nikkhah Bahrami
2021-current Shaoor Munir
2021-current Yash Vekaria
2021-current Hari Venugopalan (co-advised with Sam King)
2016-2021 Dr. Umar Iqbal; First Position: CIFellow/Postdoc, University of Washington
2015-2021 Dr. Shehroze Farooqi; First Position: Researcher, Palo Alto Networks
2015-2019 Dr. Huyen Le; First Position: Postdoc, National Center for Toxicological Research

Select Recent Masters Mentees

2021 Mohammad Ismail Daud
2021 Sunshine Chong
2021 Rachit Dhamija
2020 Pouneh Nikkhah Bahrami
2018 Daniel Zhou
2016-2017 Sai Kalyan Moguloju

Select Recent Undergraduate Mentees

2023 Divya Raj
2023 Shuaib Ahmed
2023 Ryan Swift
2023 Tangbaihe Wang
2023 Patrick Lee

2022 Jake Smith
2022 Christina Phan
2022 Kev Rockwell
2020-2022 Kajal Patel (NSF REU)
2020-2022 Wanyue Zhai (graduate student at Stanford)
2020-2022 Ray Ngan (NSF REU) (industry: Palo Alto Networks)
2020-2021 Surya Konkimalla
2020-2021 Charles Nguyen (industry: Apple)
2019-2021 Charlie Wolfe (NSF REU) (industry: Apple)
2021 Caelan MacArthur (NSF DREU)
2020-2021 Taimur Kashif (NSF REU) (industry: VMWare)
2019-2020 Ashton Woiwood (NSF REU)
2018 Basil Chatha
2017 Treyton Krupp (NSF REU)
2017 Daniel Zhou (NSF REU)
2017 Gabriel Akanni (SROP)
2016-2017 Xiaoye Li (NSF REU)
2016 Yu Dai

High School

2023 Reeva Rao
2023 Jayalakshmi Raffill
2019 Kathy Zhong
2018 Alice Martynova
2017 William Kim
2016 Brandon Wang

External Service

Conference TPC/Reviewer IEEE S&P (2022), PETS (2021, 2020, 2019, 2018, 2017), ACM IMC (2021, 2020), ACM CoNEXT (2019), ACM SIGMETRICS (2023, 2022, 2020, 2013), WWW (2020, 2018), ACM CSCW (2018, 2019), IEEE/IFIP TMA (2020, 2019), NDSS MADWeb Workshop (2019), IEEE INFOCOM (2017, 2015, 2010, 2009), ACM WPES (2018), IEEE S&P Consumer Protection Workshop (2021, 2020), ACM SIGCOMM Internet-QoE Workshop (2017), ACM SIGCOMM Workshop on IoT Security and Privacy (2018), WWW CyberSafety Workshop (2018), WWW Workshop on Location and the Web (2018), IEEE ICNP (2014, 2013), MASCOTS (2013), ICDCN (2017, 2018)

Journal Reviewer IEEE/ACM Transactions on Networking, ACM Transactions on the Web, IEEE Transactions on Mobile Computing, IEEE Transactions on Network and Service Management, ACM Transactions on Multimedia Computing, IEEE Transactions on Cognitive Communications and Networking, ACM SIGCOMM Computer Communication Review, Elsevier Computer Communications, Elsevier Performance Evaluation, Springer Wireless Networks

PC Co-Chair Privacy Enhancing Technologies Symposium (PETs), 2025

PC Co-Chair Privacy Enhancing Technologies Symposium (PETs), 2024

PC Co-Chair	Workshop on Technology and Consumer Protection (ConPro'23), IEEE Symposium on Security & Privacy ("Oakland")
PC Co-Chair	Workshop on Technology and Consumer Protection (ConPro'22), IEEE Symposium on Security & Privacy ("Oakland")
PC Co-Chair	Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb'23), Network and Distributed System Security Symposium (NDSS)
PC Co-Chair	Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb'22), Network and Distributed System Security Symposium (NDSS)
Publicity Co-Chair	ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT 2020)
Co-Chair	NSF NeTS Early Career Investigators Workshop 2019
PC Co-Chair	Student Workshop - ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT 2018)
PC Co-Chair	WWW 8th International Workshop on Location and the Web (LocWeb 2018)
Poster Chair	ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS 2018)
Technical Committee	Elsevier Computer Communications (2015-2019)
Guest Editor	Special Issue on Mobile Traffic Analytics, Elsevier Computer Communications (2016)
Editorial Board	Proceedings on Privacy Enhancing Technologies (PoPETs) (2019, 2020, 2021)
Panelist	NSF (2017, 2018, 2019, 2020, 2021, 2022, 2023)

Internal Service

Chair	Departmental Colloquium Series Department of Computer Science, University of California Davis, 2021-
Member	Diversity, Equity, Inclusion Committee College of Engineering, University of California Davis, 2021-2022
Committee	Departmental Graduate Committee Department of Computer Science, University of Iowa, 2019-2020
Chair	Departmental Colloquium Series Department of Computer Science, University of Iowa, 2019-2020
Member	Executive Committee, Iowa Initiative for Artificial Intelligence (IIAI) The University of Iowa, 2019-2020
Member	Department Executive Committee Department of Computer Science, The University of Iowa, 2016-2019
Member	Faculty Recruitment Committee Department of Computer Science, The University of Iowa, 2015-2020
Mentor	Black Girls Do Science College of Engineering, The University of Iowa, 2015-2016
Mentor	Iowa Edge Classroom Experience Center for Diversity and Enrichment, The University of Iowa, 2015-2018

Mentor Summer Research Opportunities Program (SROP)
Graduate College, The University of Iowa, 2017

Mentor Secondary Student Training Program (SSTP)
Belin-Blank Center, The University of Iowa, 2016-2019

Patents

USPTO 10484881 Jia Wang, Lusheng Ji, Alex X. Liu, Zubair Shafiq. Optimization of cellular network architecture based on device type-specific traffic dynamics. November 2019

USPTO 10420167 Jia Wang, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Zubair Shafiq. Cellular Connection Sharing. September 2019

Expert Testimony & Reports (in the past ten years)

4:20-cv-05146 **Calhoun v. Google** District Court, N.D. California

4:21-cv-02155 **In re Google RTB Consumer Privacy Litigation** District Court, N.D. California

3:23-cv-02431 **Doe v. Google** District Court, N.D. California

22-01-88230-D **State of Texas v. Google** District Court, Victoria County, Texas

A 2002633 **Doe v. Bon Secours Mercy Health** Court of Common Pleas, Hamilton County, Ohio

24-C-20-000591 **Doe v. Medstar Health** Circuit Court, Baltimore County, Maryland

19-2-26674-1 **Doe v. Virginia Mason** Superior Court, Washington

23CV037304 **Doe v. Family Planning Associates Medical Group** Superior Court, California

22-cv-03580 **In re Meta Pixel Healthcare Litigation** District Court, N.D. California

23OT01-0026 **Stake v. Knox** Court of Common Pleas, Knox County, Ohio

23-cv-00964 **Griffith v. TikTok** District Court, C.D. California

22STCV36304 **Doe v. Adventist** Superior Court, California

3:22-cv-07465 **Hazel v. Prudential** District Court, N.D. California

4:22-cv-04423 **Beke v. Fandom** District Court, N.D. California

3:22-cv-08981 **Lau v. Gen Digital** District Court, N.D. California

4:20-cv-00957 **State of Texas v. Google** District Court, E.D. Texas

Litigation Consulting (in the past ten years)

Bleichmar Fonti & Auld

Simmons Hanly Conroy

Lieff Cabraser Heimann & Bernstein

DiCello Levitt Gutzler

Norton Rose Fulbright

Pritzker Levine

Social Media Victims Law Center

Girard Sharp

Hammond Law

Caddell & Chapman

Whatley Kallas

Office of the Attorney General, Texas

AZA Law

Susman Godfrey